PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-274788
(43)Date of publication of application :05.10.2001

(51)Int.Cl H04L 9/08
G06F 13/00
G09C 1/00
H04L 12/18

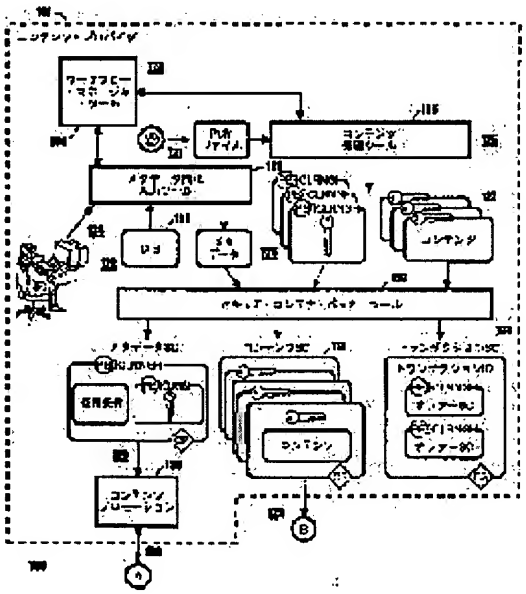
(21)Application number :2001-011996
(22)Date of filing : 19.01.2001

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : MOURAD MAGDA
MUNSON JONATHAN P
PACIFICI GIOVANNI
TANTAWY AHMED
YOUSSEF ALAA S

(30)Priority
Priority number :2000 487417 Priority date :20.01.2000 Priority country :US

(54) DISTRIBUTION OF DIGITAL CONTENTS USING WEB BROADCAST COMMUNICATION SERVICE

(57)Abstract:
PROBLEM TO BE SOLVED : To provide users with a method for surely receiving data on a system from a web broadcast communication interface through a plurality of channels.
SOLUTION : This method includes a step, where promotion meta data that are available for reception are received through a 1st web broadcast communication channel and at least part of the data is assembled into promotion offering data, a step where data to be received are selected in relation to the above data, a step where data are received from a 2nd web broadcast communication channel, a step where the data are selected from the promotion meta data and encrypted by using a 1st encryption key, and a step where a computer-readable medium receives a 1st encryption decoding key, and the decoding key is used to decode at least part of the encrypted data received from the 2nd web broadcast communication channel



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－274788
（P2001－274788A）
(43)公開日　平成13年10月５日(2001.10.5)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ	13/00	５４７Ｔ
Ｇ０６Ｆ　13/00	５４７	Ｇ０９Ｃ	1/00	６４０Ｚ
Ｇ０９Ｃ　1/00	６４０	Ｈ０４Ｌ	12/18	
Ｈ０４Ｌ　12/18			9/00	６０１Ａ
				６０１Ｂ

審査請求　有　請求項の数24　ＯＬ　（全104頁）　最終頁に続く

(21)出願番号　特願2001－11996(P2001－11996)

(22)出願日　平成13年１月19日(2001.1.19)

(31)優先権主張番号　０９／４８７４１７

(32)優先日　平成12年１月20日(2000.1.20)

(33)優先権主張国　米国（ＵＳ）

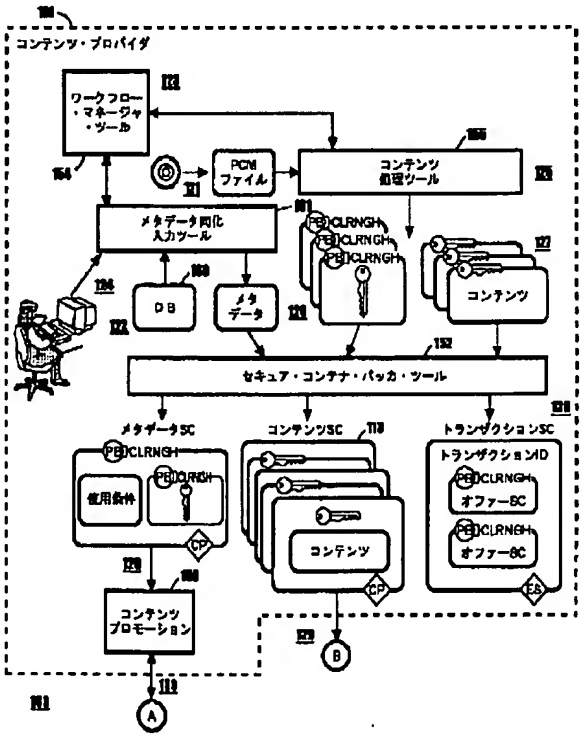
(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(74)代理人　100086243
弁理士　坂口　博　（外２名）

最終頁に続く

(54)【発明の名称】　ウェブ同報通信サービスを使用したディジタル・コンテンツの配布

(57)【要約】　（修正有）
【課題】　複数のチャネルによりウェブ同報通信インフラストラクチャからユーザのシステム上で確実にデータを受信する方法を提供する。
【解決手段】　この方法は、第１のウェブ同報通信チャネルからプロモーション・メタデータを受信するステップで又受信用に使用可能なデータに関する物のステップであり、該データの少なくとも一部をのプロモーション・オファリングにアセンブルするステップと、該データに関連して受信すべきデータを選択するステップと、第２のウェブ同報通信チャネルからデータを受信するステップであり、そのデータがプロモーション・メタデータから選択されたもので、第１の暗号化キーにより暗号化されているステップと、コンピュータ可読媒体により第１の暗号化解除キーを受信するステップであって、該解除キーが第２のウェブ同報通信チャネルにより受信したデータの少なくとも一部を暗号化解除するためのものであるステップとを含む。



【特許請求の範囲】
【請求項１】複数のチャネルを備えたウェブ同報通信インフラストラクチャによりユーザのシステムに確実にデータを提供する方法であって、
第１の暗号化キーを使用してデータを暗号化するステップと、
第２の暗号化キーを使用して第１の暗号化解除キーを暗号化するステップと、
少なくともユーザのシステム上で受信するために第１のウェブ同報通信チャネル上で暗号化データの少なくとも一部に関連するプロモーション・メタデータを同報通信するステップと、
第２の同報通信チャネルにより暗号化データの少なくとも一部を同報通信するステップと、
暗号化した第１の暗号化解除キーをコンピュータ可読媒体によりユーザのシステムに転送するステップであって、その暗号化した第１の暗号化解除キーが第２の暗号化キーによって暗号化されているステップとを含む方法。
【請求項２】プロモーション・メタデータを同報通信するステップが、所定の時間間隔で定期的にプロモーション・メタデータを同報通信することを含む、請求項１に記載の方法。
【請求項３】プロモーション・メタデータを同報通信するステップが、
少なくともプロモーション・メタデータをウェブ・ブラウザにより読取り可能なフォーマットに変換するサブステップを含む、請求項１に記載の方法。
【請求項４】暗号化データの少なくとも一部を同報通信するステップが、暗号化データの少なくとも一部に関する同報通信時間およびウェブ同報通信チャネルのスケジュールを同報通信することを含む、請求項１に記載の方法。
【請求項５】第２のウェブ同報通信チャネルにより暗号化データの少なくとも一部を同報通信するステップが、DirecPCTMと互換性のあるフォーマットで暗号化データを同報通信することを含む、請求項１に記載の方法。
【請求項６】プロモーション・メタデータがそのデータに関する同報通信時間のスケジュールを含む、請求項１に記載の方法。
【請求項７】複数のチャネルによりウェブ同報通信インフラストラクチャからユーザのシステム上で確実にデータを受信する方法であって、
第１のウェブ同報通信チャネルからプロモーション・メタデータを受信するステップであって、そのプロモーション・メタデータが受信用に使用可能なデータに関するメタ・データであるステップと、
プロモーション・メタデータの少なくとも一部をユーザによる検討用のプロモーション・オファリングにアセンブルするステップと、
プロモーション・メタデータに関連して受信すべきデータをユーザによって選択するステップと、
第２のウェブ同報通信チャネルからデータを受信するステップであって、そのデータがプロモーション・メタデータから選択されたデータであり、そのデータが第１の暗号化キーを使用してあらかじめ暗号化されているステップと、
コンピュータ可読媒体により第１の暗号化解除キーを受信するステップであって、その第１の暗号化解除キーが第２のウェブ同報通信チャネルにより受信したデータの少なくとも一部を暗号化解除するキーであるステップとを含む方法。
【請求項８】プロモーション・データの少なくとも一部をアセンブルするステップが、プロモーション・データの少なくとも一部をウェブ・ブラウザにより読取り可能なフォーマットにアセンブルすることを含み、選択するステップが、ウェブ・ブラウザにより選択することを含む、請求項７に記載の方法。
【請求項９】選択するステップが、ユーザのシステム上であらかじめ受信され記憶されたプロモーション素材を選択することを含む、請求項７に記載の方法。
【請求項１０】選択するステップが、
選択したデータの次のウェブ同報通信に関するスケジュールを決定するサブステップと、
ユーザのシステムを起動して第２のチャネル上で次のウェブ同報通信を受信するトリガを設定するサブステップとをさらに含む、請求項９に記載の方法。
【請求項１１】第２のウェブ同報通信チャネルからデータを受信するステップが、トリガによって提供されたウェブ同報通信チャネルおよび時間においてプロモーション・メタデータから選択したデータを受信することを含む、請求項１０に記載の方法。
【請求項１２】第２のウェブ同報通信チャネルからデータを受信するステップが、DirecPCTMと互換性のあるフォーマットでデータを受信することを含む、請求項７に記載の方法。
【請求項１３】第２のウェブ同報通信チャネルからデータを受信するステップが、
ユーザのシステムが選択したデータを受信することを許可されていることをバック・チャネルにより認可するサブステップを含み、第１の暗号化解除キーを受信するステップが、ユーザのシステムが選択したデータを受信することを許可されている場合にのみ第１の暗号化解除キーを受信することを含む、請求項７に記載の方法。
【請求項１４】第２のウェブ同報通信チャネルからデータを受信するステップが、
プロモーション・メタデータから選択したデータがユーザのシステム上で受信された場合に、次にユーザがユーザのシステムを始動するときにユーザに状況を通知するサブステップをさらに含む、請求項７に記載の方法。

【請求項１５】第１の暗号化解除キーを受信するステップが、第２の暗号化キーにより暗号化された第１の暗号化解除キーを受信することを含む、請求項７に記載の方法。
【請求項１６】第１の暗号化解除キーを受信するステップが、同報通信ストリームにより第１の暗号化解除キーを受信することを含む、請求項１５に記載の方法。
【請求項１７】第２の暗号化解除キーがクリアリングハウスからユーザのシステムに送信される、請求項１５に記載の方法。
【請求項１８】第２の暗号化解除キーが、クリアリングハウスからユーザのシステムに送信された第２の暗号化キーにより暗号化されたデータを暗号化解除するタイムアウト設備を有する、請求項１５に記載の方法。
【請求項１９】複数のチャネルを備えたウェブ同報通信インフラストラクチャによりユーザのシステムに確実にデータを提供するシステムであって、
コンテンツ・システムと、
第１の公開キーと、
第１の公開キーに対応する第１の秘密キーと、
データ暗号化キーと、
データ暗号化キーを使用して暗号化したデータを暗号化解除するデータ暗号化解除キーと、
データ暗号化解除キーのみによって暗号化解除可能になるようにデータを暗号化する第１のデータ暗号化手段と、
データ暗号化解除キーを暗号化するために第１の公開キーを使用する第２のデータ暗号化手段と、
クリアリング・ハウスと、
第２のウェブ同報通信チャネル上で同報通信されるデータに関連するプロモーション・データを第１のウェブ同報通信チャネル上の１つまたは複数のユーザのシステムに同報通信し、データ暗号化キーにより暗号化したデータを第２の同報通信チャネル上で同報通信する同報通信センタと、
暗号化されたデータ暗号化解除キーをクリアリング・ハウスに転送する第１の転送手段であって、クリアリング・ハウスが第１の秘密キーを所有する第１の転送手段と、
第１の秘密キーを使用してデータ暗号化解除キーを暗号化解除する第１の暗号化解除手段と、
第２の公開キーと、
第２の公開キーに対応する第２の秘密キーと、
第２の公開キーを使用してデータ暗号化解除キーを再暗号化する再暗号化手段と、
再暗号化されたデータ暗号化解除キーをユーザのシステムに転送する第２の転送手段であって、ユーザのシステムが第２の秘密キーを所有する第２の転送手段と、
第２の秘密キーを使用して再暗号化したデータ暗号化解除キーを暗号化解除する第２の暗号化解除手段とを含むシステム。
【請求項２０】プロモーション・メタデータがそのデータに関する同報通信時間のスケジュールを含む、請求項１９に記載のシステム。
【請求項２１】複数のチャネルによりウェブ同報通信インフラストラクチャから確実にデータを受信する、ユーザのシステムであって、
第１のウェブ同報通信チャネルからプロモーション・メタデータを受信する受信機であって、そのプロモーション・メタデータが受信用に使用可能なデータに関するメタデータである受信機と、
プロモーション・メタデータの少なくとも一部をユーザによる検討用に提示する出力装置へのインタフェースと、
プロモーション・メタデータに関連して受信すべきデータに関するユーザによる選択を受信する入力装置へのインタフェースと、
第２のウェブ同報通信チャネルからデータを受信するよう受信機を制御する制御装置であって、そのデータがプロモーション・メタデータから選択されたデータであり、そのデータが第１の暗号化キーを使用してあらかじめ暗号化されている制御装置と、
コンピュータ可読媒体により第１の暗号化解除キーを受信するインタフェースであって、その第１の暗号化解除キーが第２のウェブ同報通信チャネルにより受信したデータの少なくとも一部を暗号化解除するキーであるインタフェースとを含むユーザのシステム。
【請求項２２】出力装置がウェブ・ブラウザであり、入力装置がユーザによる選択を受信するためにウェブ・ブラウザに結合されている、請求項２１に記載のユーザのシステム。
【請求項２３】制御装置が、プロモーション・メタデータから導出したスケジュールであって、第２のウェブ同報通信チャネルからデータを受信するよう受信機を制御するために使用するスケジュールをさらに含む、請求項２１に記載のユーザのシステム。
【請求項２４】受信機が、DirecPCTMと互換性のあるフォーマットで同報通信されたデータを受信するよう適合されている、請求項２１に記載のユーザのシステム。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】開示する本発明は、概してエレクトロニック・コマースの分野に関し、より詳細には、インターネット、ワールド・ワイド・ウェブ、ケーブルまたは衛星ディジタル放送網などのグローバル通信ネットワークによる印刷媒体、フィルム、ゲーム、音楽などのディジタル資産の安全な送達および権利管理のためのシステムおよび関連ツールに関する。
【０００２】
【従来の技術】音楽、フィルム、コンピュータ・プログ

ラム、ピクチャ、ゲーム、その他のコンテンツなどのディジタル資産の配布のためのインターネットなどのグローバル配布システムの使用は増大し続けている。同時に、貴重なディジタル・コンテンツのオーナまたは発行者は、いくつかの理由により、ディジタル資産の配布のためのインターネットの使用になかなか取り組めなかった。理由の１つは、オーナがディジタル・コンテンツの無許可コピーまたは海賊版作成を懸念していることである。ディジタル・コンテンツの電子送達により、海賊版作成に対するいくつかのバリアが取り除かれる。電子配布によって取り除かれるバリアの１つは、有形の記録可能媒体そのもの（たとえば、ディスケットまたはＣＤ－ＲＯＭ）が必要なことである。多くの場合、ブランク・テープまたは記録可能ＣＤは１ドル未満であっても、ディジタル・コンテンツを有形媒体にコピーするには、お金が必要である。しかし、電子配布の場合、有形媒体はもはや不要である。コンテンツは電子的に配布されるので、有形媒体のコストは要因ではなくなる。第２のバリアはコンテンツ自体のフォーマットであり、すなわち、コンテンツは、ディジタル・フォーマットではなくアナログ・フォーマットで記憶されている。アナログ・フォーマットで記憶されたコンテンツ、たとえば、印刷ピクチャは、写真複写によって複製したときに、そのコピーはオリジナルより品質が悪くなる。コピーのその後の各コピーは、生成と呼ばれることもあり、コピーのたびにオリジナルより品質が悪くなる。ピクチャがディジタルで記憶されると、このような品質の劣化は存在しない。各コピーならびにどのコピー生成も、オリジナルと同様に鮮明かつ明解なものになりうる。ディジタル・コピーが完璧であることと、コンテンツを電子式に配布し、インターネットにより広範囲にコンテンツを配布するためのコストが非常に低いことを結合した集合効果により、無許可コピーの海賊版を作成して配布することは比較的容易になる。数回のキーストロークによって、著作権侵害者は、ディジタル・コンテンツの数百部または数千部の完璧なコピーをインターネットにより送信することができる。したがって、電子式に配布されるディジタル資産の保護およびセキュリティを保証することが必要である。

【０００３】ディジタル・コンテンツのプロバイダは、コンテンツ・オーナの権利を保護する、ディジタル・コンテンツ用の安全なグローバル配布システムの確立を希望している。ディジタル・コンテンツ配布システムの確立に関する問題としては、ディジタル・コンテンツ電子配布、権利管理、資産保護のためのシステムの開発を含む。電子式に配布されるディジタル・コンテンツは、印刷媒体、フィルム、ゲーム、プログラム、テレビ、マルチメディア、音楽などのコンテンツを含む。

【０００４】電子配布システムの配備によって、ディジタル・コンテンツ・プロバイダは、即時販売報告および電子調停により支払の迅速決済を達成すると同時にコンテンツの再配布により２次財源を獲得する能力がもたらされる。電子ディジタル・コンテンツ配布システムは物理的な在庫の目減りまたは返品によって左右されないので、ディジタル・コンテンツ・プロバイダおよび小売業者は、コストの低減とマージンの改善を実現することができる。ディジタル・コンテンツ・プロバイダは、在庫の時限リリースの向上のために新しい流通経路を促進するかまたは既存の流通経路を増強することができるだろう。電子配布システムからのトランザクション・データを使用して、消費者の購入パターンに関する情報を入手すると同時に電子マーケティング・プログラムおよびプロモーションに関する即時フィードバックを提供することができるだろう。これらの目標を満たすために、ディジタル資産の保護および計量を保証しながら、ディジタル・コンテンツが電子配布モデルを使用して広範囲のユーザおよびビジネスに対してディジタル・コンテンツを使用可能にする必要がある。

【０００５】リアル・オーディオ、ＡＴ＆ＴによるＡ２Ｂ、Liquid Audio Pro Corp.によるLiquid Audio Pro、Audio SoftによるCity Music Networkなど、ディジタル・コンテンツ用のその他の市販の電子配布システムは、保護付きおよび無保護の電子ネットワークによるディジタル・データの伝送を提供する。保護付き電子ネットワークを使用すると、ディジタル・コンテンツ・プロバイダの、広範囲の視聴者にディジタルを配布する要件が大幅に低減される。インターネットおよびウェブなどの無保護ネットワークを使用すると、ディジタル・コンテンツは暗号化の使用などにより確実にエンドユーザに到着することができる。しかし、暗号化されたディジタル・コンテンツがエンドユーザのマシン上で暗号化解除されると、そのディジタル・コンテンツは無許可再配布のためにエンドユーザにとって容易に使用可能なものになる。したがって、ディジタル資産の保護を提供し、ディジタル・コンテンツが消費者およびビジネスに送達された後でもコンテンツ・プロバイダの権利が保護される、安全なディジタル・コンテンツ電子配布システムが必要になる。したがって、ディジタル資産の安全な送達、ライセンス許可、および使用制御を可能にするための権利管理が必要になる。

【０００６】ディジタル・コンテンツのオーナが電子配布になかなか取り組めなかったもう１つの理由は、既存の流通経路を維持し育成したいという彼らの希望である。ほとんどのコンテンツ・オーナは小売業者を通して販売している。音楽市場では、このような米国小売業者としては、Tower Records、Peaches、Blockbuster、Circuit Cityなどを含む。これらの小売業者の多くは、インターネット・ユーザがインターネットによって選択を行い、選択したものをエンドユーザに郵送できるようにするウェブ・サイトを有している。音楽ウェブ・サイトの

例としては、Tower、Music Boulevard、Columbia Houseを含む。電子配布を使用すると、特にウェブ上で、小売店同士が互いに区別し、小売店とコンテンツ・オーナとを区別する能力が取り除かれる可能性がある。したがって、ピクチャ、ゲーム、音楽、プログラム、ビデオなどの電子コンテンツの小売業者に対し、電子配布により音楽を販売するときに互いに区別し、小売業者とコンテンツ・オーナとを区別する方法を提供することが必要である。

【０００７】コンテンツ・オーナは、電子ストアなどの配布サイトからの電子配布用としてそれぞれのディジタル・コンテンツを作成する。インターネット上または他のオンライン・サービスによる電子ストアは、それぞれの製品オファリングおよび製品プロモーションによってストア同士を互いに区別したいと望んでいる。伝統的な店、すなわち、電子ストアに類似した非電子非オンラインの店では、製品プロモーション、製品販売、製品サンプル、自由返品方針、その他のプロモーション・プログラムを使用して、自分の店とその競合店とを区別している。しかし、コンテンツ・プロバイダがディジタル・コンテンツに使用条件を課しているオンライン世界では、電子ストアがストア同士を区別する能力は厳格に制限される場合がある。そのうえ、使用条件を変更できる場合でも、電子ストアは、電子的に製品をプロモートし販売するためにコンテンツ・プロバイダからのディジタル・コンテンツに関連するメタデータを処理するという困難な課題に直面している。電子ストアは、メタデータを処理するときにいくつかの要件を管理する必要がある。第１に、電子ストアは、コンテンツ・プロバイダからのディジタル・コンテンツに関連するメタデータを受信しなければならない。多くの場合、このメタデータの部分部分を暗号化して送信することができ、したがって、コンテンツ・プロバイダは暗号化コンテンツを暗号化解除するためのメカニズムを作成しなければならない。第２に、電子ストアは、そのコンテンツに関する製品マーケティング、製品のポジショニング、その他のプロモーション上の考慮事項を支援するために、コンテンツ・プロバイダからコンテンツを受信する前または電子ストアがコンテンツを受信した後のいずれかに、コンテンツ・プロバイダからのメタデータをあらかじめ見ておきたいと希望する場合がある。第３に、電子ストアは、グラフィックおよびアーチスト情報などのプロモーション素材に使用する所与のメタデータを抽出しなければならない。多くの場合、このプロモーション素材は、そのオンライン・プロモーションで電子ストアが直接使用する。第４に、電子ストアは、許可された使用条件の一部を変更してディジタル・コンテンツの各種オファリングを作成することにより、ストア同士を互いに区別したいと希望する場合がある。第５に、電子ストアは、支払決済のために電子ストアを通り抜ける必要なしに購入者によって自動的に会計調停ハウスに支払調停を指示するためにＵＲＬなどの所与のアドレスをメタデータに挿入するかまたは変更しなければならない場合もある。第６に、電子ストアは、使用条件と一致する、著作権で保護されたディジタル・コンテンツの許可された使用に関するライセンスを作成することが必要になる場合もある。たとえば、このライセンスでは、ディジタル・コンテンツの限られた数のコピーを作成するための許可を授与することができる。授与される許可の条件を反映するためにライセンスが必要である。

【０００８】これらすべての要件を考慮すると、ディジタル・コンテンツに関連するメタデータを処理するために、多くの電子ストアでは、これらの要件を処理するためのカストマイズ・ソフトウェア・プログラムを作成する。このようなカストマイズ・ソフトウェア・プログラムを作成するために必要な時間、コスト、およびテストは多大なものになる可能性がある。したがって、このような要件の解決策を提供することが必要である。

【０００９】さらに、ディジタル・コンテンツのオーナが電子配布になかなか取り組めなかったもう１つの理由は、電子配布用のコンテンツの作成が難しいことである。今日、多くのコンテンツ・プロバイダは、そのポートフォリオに数千または数万タイトルを有している。音楽の例では、同時に数通りのフォーマット（たとえば、ＣＤ、テープ、ミニディスク）で使用可能な単一マスタ録音をコンテンツ・オーナが有していることは珍しいことではない。そのうえ、単一フォーマットは、特定の流通経路用にマスタを新たに作成したかまたはリミックスしたマスタ録音を有する可能性もある。一例として、ラジオ放送用のミキシングはダンス・クラブのサウンド・トラック用のミキシングとは異なる場合があり、ダンス・クラブのサウンド・トラックは一般に使用可能な消費者用ＣＤとは異なる場合がある。このような様々なミキシングの目録を作成し、追跡することは厄介なものになる可能性がある。しかも、マスタ録音の多くのオーナは、「ベスト盤」など様々な後続コレクションまたは映画に合わせた音楽サウンド・トラックの編集物、その他のコレクションまたは編集物で古い録音を再発行する場合が多い。ディジタルで提供されるコンテンツが増えるにつれて、電子配布用のコンテンツをリミックスし、コード化する必要性が増大する。多くの場合、プロバイダは、正しいマスタ録音を選択するためのガイドとして古い記録フォーマットを使用し、電子配布用のリリースのためにこれらの録音を再処理しコード化させる必要がある。これは、特に、その古いフォーマットを使用して電子配布のために古い録音をリリースし直すのを支援したいと希望するコンテンツ・プロバイダに当てはまる可能性がある。プロバイダは、データベースを調べてタイトル、アーチスト、録音を突き合わせ、コード化パラメータを設定することになる。記録ポートフォリオを求めて

データベースを手動でサーチするこのプロセスは、欠点がないわけではない。１つの欠点は、オペレータが手動でデータベースをサーチして、処理パラメータを適切にセットする必要があることである。もう１つの欠点は、データベースからデータを選択する際にオペレータの転記エラーが発生する可能性があることである。したがって、音声などのコンテンツに関する関連データおよびマスタ記録を自動的に検索するための方法をコンテンツ・プロバイダに提供することが必要である。

【００１０】コンテンツ・オーナは、コード化として知られるプロセスにより、電子配布用のディジタル・コンテンツを作成する。コード化は、コンテンツを取得することと、そのコンテンツがアナログ・フォーマットで提示されている場合はそれをディジタル化することと、さらにそれを圧縮することを含む。伝送または記憶されるデータの量が低減されるので、圧縮するプロセスにより、ディジタル・コンテンツはネットワークによって転送することができ、より効率よく記録可能媒体に記憶することができる。しかし、圧縮には欠点がないわけではない。ほとんどの圧縮は何らかの情報の損失を伴い、損失圧縮と呼ばれる。コンテンツ・プロバイダは、どの圧縮アルゴリズムを使用するかと、必要な圧縮レベルを決定しなければならない。たとえば、音楽では、ディジタル・コンテンツまたはディジタル歌曲は、音楽のジャンルに応じて非常に異なる特性を有する可能性がある。あるジャンルについて選択された圧縮アルゴリズムおよび圧縮レベルは、他のジャンルの音楽には最適な選択ではない可能性がある。また、コンテンツ・プロバイダは、圧縮・アルゴリズムと圧縮レベルの所与の組合せがあるジャンルの音楽、たとえばクラシックには非常にうまく機能するが、ヘビー・メタルなどの他のジャンルの音楽には不満足な結果をもたらすことに気づく可能性がある。そのうえ、オーディオ・エンジニアは、音楽を等化し、ダイナミック・レンジ調整を実行し、他の前処理および処理設定を実行して、コード化した音楽のジャンルが所望の結果をもたらすことを保証しなければならない。各ディジタル・コンテンツごとの等化レベルおよびダイナミック・レンジ設定など、これらのコード化パラメータをいつも手動で設定しなければならないという要件は、厄介なものになる可能性がある。音楽の例に戻ると、様々な音楽ジャンルをカバーするコレクションを伴う音楽のコンテンツ・プロバイダは、コード化すべき各歌曲または各歌曲セットごとにコード化パラメータの所望の組合せを手動で選択しなければならないだろう。したがって、コード化のためのプロセス・パラメータの手動選択の必要性を克服することが必要である。

【００１１】

【発明が解決しようとする課題】コンテンツを圧縮するためのプロセスは、特に長篇特作映画などの大型コンテンツ項目の場合、大量の専用計算リソースを必要とする可能性がある。圧縮アルゴリズムのプロバイダは、自身の圧縮技法に関連する様々な兼ね合いおよび利点を提示している。これらの兼ね合いとしては、コンテンツを圧縮するために必要な時間および計算リソースの量、元のコンテンツから達成される圧縮の量、再生のための所望のビット伝送速度、圧縮したコンテンツのパフォーマンス品質、その他の要因を含む。入力としてマルチメディア・ファイルを取り入れ、コード化した出力ファイルを生成し、経過および状況の中間表示を一切行わないコード化プログラムを使用することは問題である。しかも、多くの状況では、経過の中間表示を一切行わないコード化プログラムを呼び出すかまたはそれを管理するために、他のプログラムを使用する。このため、呼出しアプリケーションには、コード化すべきものとして指定された選択内容全体のパーセンテージとして、コード化されたコンテンツの量を測定する方法は一切残されない。呼出しプログラムが一度に実行するよう数通りのプログラムをスケジューリングしようと試みる状況では、これは問題になる可能性がある。さらに、コード化のためにコンテンツ・バッチが選択され、コンテンツ・プロバイダがコード化プロセスの経過を判定したいと希望する場合、これは特に厄介なものになる可能性がある。したがって、このような問題を克服することが必要である。

【００１２】ディジタル・コンテンツ・プロバイダが自身のコンテンツのために電子配布をなかなか採用しなかったさらにもう１つの理由は、電子的に送達されたコンテンツ用としてエンドユーザ装置上のディジタル・プレーヤを作成するための標準がなかったことである。コンテンツ・プロバイダ、電子ストア、電子配布チェーン内のその他のものは、ＰＣ、セットトップ・ボックス、ハンドヘルド装置などの様々な装置上でカストマイズ・プレーヤを提供したいと希望している可能性がある。改竄防止環境、すなわち、第三者による再生中にコンテンツへの無許可アクセスを阻止するための環境でディジタル・コンテンツの暗号化解除を処理できる１組のツールが必要である。そのうえ、購入したもの以外の用途でエンド・ユーザがコンテンツにアクセスできないようにして、エンド・ユーザがディジタル・コンテンツのローカル・ライブラリを管理できるようにする１組のツールが必要である。

【００１３】ディジタル・コンテンツ・プロバイダがディジタル・コンテンツのオンライン配布をなかなか採用しなかったさらにもう１つの理由は、圧縮済みであってもコンテンツを標準の電話回線によって送達するために要する時間である。既存の同報通信インフラストラクチャによりディジタル・コンテンツのダウンロードを可能にする、Intel Intellicastシステムや「Hughes DirecPC」など、同報通信インフラストラクチャにより情報を提供するためのその他のシステムが存在する。これらの同報通信システムは、有用ではあるが、欠点がないわけ

ではない。まず初めに、これらのシステムは、ディジタル・コンテンツの配布のために安全な環境を提供しない。今日使用可能なシステムの多くは、所望のディジタル・コンテンツを選択するために、通常は電話回線であるバック・チャネルを使用する必要がある。バック・チャネルまたは電話回線が使用不能である場合、そのコンテンツは選択することができない。その他のシステムは、単一ディジタル・チャネルでプロモーション・データ、コンテンツ・データ、メタデータを提供するわけではなく、むしろ、これらの機能の１つまたは複数のために追加の両方向チャネルを必要とする。本発明では、ダウンロードオンデマンドならびに破壊されたコンテンツ・データ・ブロックの効率の良い再伝送のために、それが使用可能であれば両方向チャネルを使用することができる。したがって、この欠点を克服することが必要である。

【００１４】現行同報通信システムのもう１つの欠点は、通信回線、同報通信インフラストラクチャ、ＤＶＤおよびＣＤなどのコンピュータ可読媒体によりコンテンツを確実に配布するためにコンテンツのプロバイダが同一ツールを使用できないことである。したがって、これらの問題を克服するために同報通信インフラストラクチャによりディジタル・コンテンツの送達を可能にするための方法およびシステムが必要である。

【００１５】ディジタル・コンテンツ保護の背景に関する詳細は、以下の３つの情報源から得られる。http://www.a2bmusic.com/about/papers/musicipp.htmというＵＲＬでオンラインで入手可能なAT&T Labs (Florham Park、N.J.) のJack Lacy、James Snyder、David Maherによる「Music on the Internet and the IntellectualProperty Protection Problem」。http://www.intertrust.com/architecture/stc.htmlというＵＲＬでオンラインで入手可能なInterTrust Technologies Corp. (Sunnyvale、CA) のOlin Silbert、David Bernstein、David Van Wieによる「Securing the Content, Not the Wire for Information Commerce」という記事に記載されたDigiBoxという暗号保護コンテナ。http://cyptolope.ibm.com/white.htmというＵＲＬでオンラインで入手可能な「Cryptolope Container Technology」というIBM White Paper。

【００１６】

【課題を解決するための手段】複数のチャネルによりウェブ同報通信インフラストラクチャからユーザのシステム上で確実にデータを受信する方法である。この方法は、第１のウェブ同報通信チャネルからプロモーション・メタデータを受信するステップであって、そのプロモーション・メタデータが受信用に使用可能なデータに関するものであるステップと、プロモーション・メタデータの少なくとも一部をユーザによる検討用のプロモーション・オファリングにアセンブルするステップと、プロモーション・メタデータに関連して受信すべきデータをユーザによって選択するステップと、第２のウェブ同報通信チャネルからデータを受信するステップであって、そのデータがプロモーション・メタデータから選択されたものであり、そのデータが第１の暗号化キーを使用してあらかじめ暗号化されているステップと、コンピュータ可読媒体により第１の暗号化解除キーを受信するステップであって、その第１の暗号化解除キーが第２のウェブ同報通信チャネルにより受信したデータの少なくとも一部を暗号化解除するためのものであるステップとを含む。

【００１７】他の実施形態では、ウェブ同報通信センタから確実にデータを伝送するための方法およびシステムを開示する。

【００１８】

【発明の実施の形態】本実施形態の各項を迅速に突き止めるのを支援するために、本発明に関する目次を示す。

【００１９】Ｉ．セキュア・ディジタル・コンテンツ電子配布システム

Ａ．システム概要

１．権利管理

２．計量

３．オープン・アーキテクチャ

Ｂ．システム機能要素

１．コンテンツ・プロバイダ

２．電子ディジタル・コンテンツ・ストア

３．中間市場パートナ

４．クリアリング・ハウス

５．エンドユーザ装置

６．伝送インフラストラクチャ

Ｃ．システム用途

II．暗号概念およびセキュア・ディジタル・コンテンツ電子配布システムへの応用

Ａ．対称アルゴリズム

Ｂ．公開キー・アルゴリズム

Ｃ．ディジタル・シグニチャ

Ｄ．ディジタル証書

Ｅ．ＳＣ図形表現のガイド

Ｆ．セキュア・コンテナ暗号化の例

III．セキュア・ディジタル・コンテンツ電子配布システムのフロー

IV．権利管理アーキテクチャ・モデル

Ａ．アーキテクチャ層機能

Ｂ．機能区分およびフロー

１．コンテンツ・フォーマット層

２．コンテンツ使用制御層

３．コンテンツ識別層

４．ライセンス制御層

Ｃ．コンテンツ配布ライセンス制御

Ｖ．セキュア・コンテナ構造

A．一般構造
B．権利管理言語構文およびセマンティクス
C．セキュア・コンテナのフローおよび処理の概要
D．メタデータ・セキュア・コンテナ６２０のフォーマット
E．オファー・セキュア・コンテナ６４１のフォーマット
F．トランザクション・セキュア・コンテナ６４０のフォーマット
G．オーダ・セキュア・コンテナ６５０のフォーマット
H．ライセンス・セキュア・コンテナ６６０のフォーマット
I．コンテンツ・セキュア・コンテナのフォーマット
VI．セキュア・コンテナのパックおよびアンパック
A．概要
B．素材一覧表（ＢＯＭ）パーツ
C．キー記述パーツ
VII．クリアリング・ハウス
A．概要
B．権利管理処理
C．国別固有パラメータ
D．監査ログおよび追跡
E．結果の報告
F．請求および支払検証
G．再伝送
VIII．コンテンツ・プロバイダ
A．概要
B．ワーク・フロー・マネージャ
１．製品待受けアクション／情報プロセス
２．新コンテンツ要求プロセス
３．自動メタデータ収集プロセス
４．手動メタデータ入力プロセス
５．使用条件プロセス
６．監視付きリリース・プロセス
７．メタデータＳＣ作成プロセス
８．ウォータマーク・プロセス
９．前処理圧縮プロセス
１０．コンテンツ品質管理プロセス
１１．暗号化プロセス
１２．コンテンツＳＣ作成プロセス
１３．最終品質保証プロセス
１４．コンテンツ分散プロセス
１５．ワーク・フロー規則
C．メタデータ同化入力ツール
１．自動メタデータ収集ツール
２．手動メタデータ入力ツール
３．使用条件ツール
４．メタデータＳＣの各パーツ
５．監視付きリリース・ツール
D．コンテンツ処理ツール
１．ウォータマーク・ツール
２．前処理圧縮ツール
３．コンテンツ品質管理ツール
４．暗号化ツール
E．コンテンツＳＣ作成ツール
F．最終品質保証ツール
G．コンテンツ分散ツール
H．コンテンツ・プロモーション・ウェブ・サイト
I．コンテンツ・ホスト
１．コンテンツ・ホスト・サイト
２．セキュア・ディジタル・コンテンツ電子配布システムによって提供されるコンテンツ・ホスト・サイト１１１
IX．電子ディジタル・コンテンツ・ストア
A．概要ー複数電子ディジタル・コンテンツ・ストアのサポート
B．ポイントツーポイント電子ディジタル・コンテンツ配布サービス
１．統合要件
２．コンテンツ収集ツール
３．トランザクション処理モジュール
４．通知インタフェース・モジュール
５．会計調停ツール
C．同報通信電子ディジタル・コンテンツ配布サービス
１．マルチティア・ディジタルＴＶの実施形態
２．個別チャネルによるウェブ同報通信の実施形態
X．エンドユーザ装置
A．概要
B．アプリケーションのインストール
C．セキュア・コンテナ・プロセッサ
D．プレーヤ・アプリケーション
１．概要
２．エンドユーザ・インタフェース・コンポーネント
３．コピー／再生管理コンポーネント
４．暗号化解除１５０５、圧縮解除１５０６、再生の各コンポーネント
５．データ管理１５０２およびライブラリ・アクセスの各コンポーネント
６．アプリケーション間通信コンポーネント
７．その他の各種コンポーネント
８．汎用プレーヤ
E．同報通信送達モードのエンドユーザ装置１０９
１．マルチティア・ディジタルＴＶの実施形態
個別チャネルによるウェブ同報通信の実施形態
【００２０】I．セキュア・ディジタル・コンテンツ電子配布システム
A．システム概要
セキュア・ディジタル・コンテンツ電子配布システムは、エンドユーザ・クライアント装置へのディジタル・コンテンツおよびディジタル・コンテンツ関連コンテン

ツの安全な送達および権利管理に必要な技術、仕様、ツール、ソフトウェアを包含する技術プラットフォームである。エンドユーザ装置としては、ＰＣ、セット・トップ・ボックス（ＩＲＤ）、インターネット家電を含む。これらの装置は、コンテンツ所有者によって許可された外部媒体または携帯用消費者装置にそのコンテンツをコピーすることができる。ディジタル・コンテンツまたは単にコンテンツという用語は、ディジタル・フォーマットで記憶された情報およびデータを意味し、ピクチャ、映画、ビデオ、音楽、プログラム、マルチメディア、ゲームを含む。

【００２１】この技術プラットフォームは、どのようにしてディジタル・コンテンツを作成し、エンドユーザ装置にライセンスされたポイントツーポイント・インフラストラクチャおよび同報通信インフラストラクチャ（ケーブル、インターネット、衛星、無線など）により確実に配布し、無許可コピーまたは再生から保護するかを指定するものである。そのうえ、この技術プラットフォームのアーキテクチャは、それらが経時的に進化するにつれて、ウォータマーク、圧縮／コード化、暗号化、その他のセキュリティ・アルゴリズムなどの様々な技術の統合および移行を可能にする。

【００２２】セキュア・ディジタル・コンテンツ電子配布システムのベース・コンポーネントは、（１）コンテンツ所有者の所有権の保護のための権利管理と、（２）即時および正確な補償のためのトランザクション計量と、（３）コンテンツ・プロバイダがコンテンツを作成し、任意の規格適合プレーヤで再生するために複数のネットワーク・インフラストラクチャによるその安全な送達を許可できるようにする、オープンかつ文書による十分な裏づけのあるアーキテクチャである。

【００２３】１．権利管理

セキュア・ディジタル・コンテンツ電子配布システムにおける権利管理は、システムの動作コンポーネント間に分散された１組の機能によって実施される。その１次機能としては、ライセンスを確保した許可中間ユーザまたはエンドユーザだけがコンテンツをロック解除するようにするライセンス許可および制御と、許可されたコピー数、再生回数、そのライセンスが有効である時間間隔または期間など、購入またはライセンスの条件に応じたコンテンツ使用の制御および執行を含む。権利管理の２次機能は、コンテンツの無許可コピーの発生源を識別するための手段によって著作権侵害と闘えるようにすることである。

【００２４】ライセンス許可および制御は、クリアリング・ハウスエンティティとセキュア・コンテナ（ＳＣ）技術の使用によって実施される。クリアリング・ハウスは、中間ユーザまたはエンドユーザがライセンス・トランザクションの正常終了を検証した後でコンテンツをロック解除できるようにすることによってライセンス許可を可能にする。セキュア・コンテナは、暗号化したコンテンツおよび情報をシステム・コンポーネント間に分散するために使用する。ＳＣは、電子情報およびコンテンツに対する無許可インターセプトまたは変更から保護するために暗号化、ディジタル・シグニチャ、ディジタル証書を使用する情報またはコンテンツの暗号キャリアである。また、これは、ディジタル・コンテンツの信憑性および完全性の検証も可能にする。これらの権利管理機能の利点は、ディジタル・コンテンツの電子配布インフラストラクチャが安全であるかまたは信頼できるものである必要がないことである。したがって、ウェブおよびインターネットなどのネットワーク・インフラストラクチャによる伝送が可能になる。これは、コンテンツがセキュア・コンテナ内で暗号化され、その記憶および配布がそのロック解除および使用の制御から切り離されているという事実による。暗号化解除キーを有するユーザだけが暗号化コンテンツをロック解除することができ、クリアリング・ハウスは許可された適切な使用要求についてのみ暗号化解除キーをリリースする。クリアリング・ハウスは、未知または無許可の当事者からの偽要求またはコンテンツ所有者が設定したコンテンツの使用条件に適合しない要求をクリアしなくなる。そのうえ、その伝送中にＳＣが改竄された場合、クリアリング・ハウス内のソフトウェアは、ＳＣ内のコンテンツが破壊または変造されたと判断し、そのトランザクションを拒絶する。

【００２５】コンテンツの使用制御は、エンドユーザ装置上で実行されるエンドユーザ・プレーヤ・アプリケーション１９５によって可能になる。このアプリケーションは、２次コピーおよび再生の許容数を定義するディジタル・コードをコンテンツのすべてのコピーに埋め込む。このディジタル・コードを生成し、それを他のエンドユーザ・プレーヤ・アプリケーション１９５から隠された状態で保持し、それを変更試行に耐えられるものにするために、ディジタル・ウォータマーク技術を使用する。代替実施形態では、このディジタル・コードは、コンテンツ１１３に関連する使用条件の一部として保持されるだけである。適合エンドユーザ装置内でディジタル・コンテンツ１１３にアクセスすると、エンドユーザ・プレーヤ・アプリケーション１９５はそのウォータマークを読み取って用途制限をチェックし、必要に応じてそのウォータマークを更新する。要求されたコンテンツの用途が使用条件に適合しない場合、たとえば、コピー数を使い果たしている場合、エンドユーザ装置はその要求を実行しなくなる。

【００２６】ディジタル・ウォータマークは、コンテンツの許可コピーまたは無許可コピーの発生源を識別するための手段も提供する。コンテンツ内の初期ウォータマークは、コンテンツ所有者を識別し、著作権情報を指定し、配布地域を定義し、その他の関連情報を追加するために、コンテンツ所有者によって埋め込まれる。第２の

ウォータマークは、コンテンツ購入者（またはライセンス保持者）およびエンドユーザ装置を識別し、購入またはライセンス条件および日付を指定し、その他の関連情報を追加するために、エンドユーザ装置側でコンテンツ内に埋め込まれる。

【００２７】ウォータマークはコンテンツの一体部分になるので、コピーが許可されているかどうかとは無関係に、コピーで伝達される。したがって、ディジタル・コンテンツは、コンテンツがどこに存在するかまたはどこから来たかにかかわらず、そのソースおよびその許可用途に関する情報を必ず含んでいる。この情報は、コンテンツの違法使用と闘うために使用することができる。

【００２８】２．計量

その権利管理機能の一部として、クリアリング・ハウスは、クリアリング・ハウスによりキー交換がクリアされるすべてのトランザクションを記録する。この記録により、ライセンス許可と元の使用条件の計量が可能になる。トランザクション記録は、取引の支払およびその他の使用の電子調停を容易にするために即時または定期的にコンテンツ所有者またはコンテンツ・プロバイダ、小売業者、その他などの担当当事者に報告することができる。

【００２９】３．オープン・アーキテクチャ

セキュア・ディジタル・コンテンツ電子配布システム（システム）は、コンテンツ所有者のための権利保護を維持しながら市場におけるシステムの幅広い実施と受入れを容易にするために、仕様書およびインタフェースを備えたオープン・アーキテクチャである。システム・アーキテクチャの柔軟性と開放性により、システムは、様々な技術、伝送インフラストラクチャ、装置が市場に送達されるにつれて、経時的に進化することもできる。

【００３０】このアーキテクチャは、コンテンツの性質とそのフォーマットの点ではオープンである。オーディオ、プログラム、マルチメディア、ビデオ、その他のタイプのコンテンツの配布は、このアーキテクチャによってサポートされる。コンテンツは、ディジタル音楽用のリニアＰＣＭなどの固有フォーマットか、またはフィルタリング、圧縮、プリエンファシス／デエンファシスなどの追加の前処理またはコード化によって達成されるフォーマットにすることができるだろう。このアーキテクチャは、様々な暗号化およびウォータマーク技法にとってオープンなものである。これは、様々なコンテンツ・タイプおよびフォーマットに対処し、それらが進化するにつれて新しい技術の導入または採用を可能にするために、特定の技法の選択を可能にする。この柔軟性により、コンテンツ・プロバイダはセキュア・ディジタル・コンテンツ電子配布システム内でデータ圧縮、暗号化、およびフォーマットのために使用する技術を選び出し、進化させることができる。

【００３１】また、このアーキテクチャは、様々な配布ネットワークおよび配布モデルにとってもオープンなものである。このアーキテクチャは、低速インターネット接続または高速衛星およびケーブル・ネットワークによるコンテンツ配布をサポートし、ポイントツーポイント・モデルまたは同報通信モデルとともに使用することができる。そのうえ、このアーキテクチャは、低コスト消費者装置を含む多種多様な装置上でエンドユーザ装置内の諸機能を実施できるように設計されている。この柔軟性により、コンテンツ・プロバイダおよび小売業者は多様なサービス・オファリングによって中間ユーザまたはエンドユーザにコンテンツを提供することができ、ユーザはコンテンツを購入またはライセンスし、それを再生し、それを様々な適合プレーヤ装置に記録することができる。

【００３２】Ｂ．システム機能要素

次に図１ないし図４に移行すると、本発明によるセキュア・ディジタル・コンテンツ電子配布システム１００の概要を示すブロック図が示されている。セキュア・ディジタル・コンテンツ電子配布システム１００は、エンドツーエンド・ソリューションを含む複数のビジネス要素を包含し、コンテンツ・プロバイダ（１０１）またはディジタル・コンテンツの所有者、電子ディジタル・コンテンツ・ストア１０３、中間市場パートナ（図示せず）、クリアリング・ハウス１０５、コンテンツ・ホスト・サイト１１１、伝送インフラストラクチャ１０７、エンドユーザ装置１０９を含む。これらのビジネス要素のそれぞれは、セキュア・ディジタル・コンテンツ電子配布システム１００の様々なコンポーネントを使用する。特に電子コンテンツ１１３の配布に関連するので、これらのビジネス要素とシステム・コンポーネントの高レベルの説明を以下に示す。

【００３３】１．コンテンツ・プロバイダ１０１

コンテンツ・プロバイダ１０１またはコンテンツ所有者は、元のコンテンツ１１３のオーナであるか、またはさらに配布するために独立したコンテンツ１１３をパッケージ化する権限を授与された配布者あるいはその両方である。コンテンツ・プロバイダ１０１は、自分の権利を直接活用するか、あるいは通常はエレクトロニック・コマースの収入に関するコンテンツ使用の支払と引き換えに電子ディジタル・コンテンツ・ストア１０３または中間市場パートナ（図示せず）にコンテンツ１１３をライセンスすることができる。コンテンツ・プロバイダ１０１の例としては、ソニー、タイムワーナー、ＭＴＶ、ＩＢＭ、マイクロソフト、ターナー、フォックスなどを含む。

【００３４】コンテンツ・プロバイダ１０１は、配布のために自分のコンテンツ１１３と関連データを作成するために、セキュア・ディジタル・コンテンツ電子配布システム１００の一部として提供されたツールを使用する。ワーク・フロー・マネージャ・ツール１５４は、処

理すべきコンテンツ１１３をスケジューリングし、高い品質保証を維持するためにコンテンツ１１３の作成およびパッケージ化の様々なステップを通過するときにコンテンツ１１３を追跡する。コンテンツ１１３に関するデータを意味するために本明細書全体を通してメタデータという用語を使用するが、この用語は本実施形態ではコンテンツ１１３そのものは含まない。一例として、歌曲のメタデータは、歌曲タイトルまたは歌曲クレジットにすることができるが、その歌曲の録音にすることはできない。コンテンツ１１３は録音を含むことになるだろう。メタデータ同化入力ツール１６１は、コンテンツ・プロバイダのデータベース１６０からのメタデータまたは規定のフォーマットでコンテンツ・プロバイダによって提供されるデータ（音楽の例の場合、ＣＤタイトル、アーチスト名、歌曲タイトル、ＣＤアートワークなどのコンテンツ１１３の情報）を抽出し、電子配布のためにそれをパッケージ化するために使用する。また、メタデータ同化入力ツール１６１は、コンテンツ１１３の使用条件を入力するためにも使用する。使用条件のデータとしては、コピー制限規則、卸売価格、必要と思われる任意のビジネス規則を含むことができる。ウォータマーク・ツールは、コンテンツ・オーナ、処理日、その他の関連データを識別するデータをコンテンツ１１３内に隠すために使用する。コンテンツ１１３がオーディオである実施形態の場合、オーディオ・プリプロセッサ・ツールを使用して、最適圧縮品質のために強弱の変化を調節するかあるいはコンテンツ１１３またはその他のオーディオを等化し、所望の圧縮レベルまでコンテンツ１１３を圧縮し、コンテンツ１１３を暗号化する。これらは、ディジタル・コンテンツ圧縮／コード化、暗号化、フォーマット方法の技術的進歩に追随し、市場でそれらが経時的に進化するにつれてコンテンツ・プロバイダ１０１が最良のツールを使用できるように適合させることができる。

【００３５】暗号化コンテンツ１１３、ディジタル・コンテンツ関連データまたはメタデータ、暗号化キーは、ＳＣパッカ・ツールによってＳＣ（以下に記載する）内にパックされ、電子配布のためにコンテンツ・ホスト・サイトまたはプロモーション・ウェブ・サイトあるいはその両方に記憶される。コンテンツ・ホスト・サイトは、コンテンツ・プロバイダ１０１に存在するか、あるいは電子ディジタル・コンテンツ・ストア１０３および中間市場パートナ（図示せず）設備を含む複数の位置に存在する可能性がある。コンテンツ１１３とキー（以下に記載する）はいずれも暗号化され、ＳＣ内にパックされるので、電子ディジタル・コンテンツ・ストア１０３または他のホスト・エージェントは、クリアリング・ハウスからのクリアランスとコンテンツ・プロバイダ１０１への通知なしに、暗号化解除したコンテンツ１１３に直接アクセスすることはできない。

【００３６】２．電子ディジタル・コンテンツ・ストア１０３

電子ディジタル・コンテンツ・ストア１０３は、コンテンツ１１３のテーマ・プログラミングまたはコンテンツ１１３の電子マーチャンダイジングなど多種多様なサービスまたはアプリケーションによりコンテンツ１１３のマーケティングを行うエンティティである。電子ディジタル・コンテンツ・ストア１０３は、自分のサービスの設計、開発、事業計画、決済、マーチャンダイジング、マーケティング、販売を管理する。オンライン電子ディジタル・コンテンツ・ストア１０３の例は、ソフトウェアの電子ダウンロードを提供するウェブ・サイトである。

【００３７】それぞれのサービス内で電子ディジタル・コンテンツ・ストア１０３は、セキュア・ディジタル・コンテンツ電子配布システム１００の所与の機能を実施する。電子ディジタル・コンテンツ・ストア１０３は、コンテンツ・プロバイダ１０１からの情報を集め、コンテンツとメタデータを追加のＳＣ内にパックし、サービスまたはアプリケーションの一部としてそのＳＣを消費者またはビジネスに送達する。電子ディジタル・コンテンツ・ストア１０３は、セキュア・ディジタル・コンテンツ電子配布システム１００によって提供されるツールを使用して、メタデータ抽出、２次使用条件、ＳＣパッケージ化、電子コンテンツ・トランザクションの追跡を支援する。２次使用条件データとしては、コンテンツ１１３の購入価格、ペイパーリッスン価格、コピー許可、ターゲット装置タイプ、時限可用性制限などの小売業ビジネス・オファーを含むことができる。

【００３８】電子ディジタル・コンテンツ・ストア１０３がエンドユーザからの電子コンテンツ１１３を求める有効な要求を完了すると、電子ディジタル・コンテンツ・ストア１０３は、顧客にコンテンツ１１３用の暗号化解除キーをリリースする権限をクリアリング・ハウス１０５に授与する責任がある。また、電子ディジタル・コンテンツ・ストアは、コンテンツ１１３を含むＳＣのダウンロードも許可する。電子ディジタル・コンテンツ・ストアは、そのローカル・サイト側でディジタル・コンテンツを含むＳＣをホストとして処理することを選ぶか、あるいは他のコンテンツ・ホスト・サイトのホストおよび配布設備を使用することができる。

【００３９】電子ディジタル・コンテンツ・ストアは、セキュア・ディジタル・コンテンツ電子配布システム１００を使用して、エンドユーザが有する可能性のある任意の質問または問題に関する顧客サービスを提供することができるか、あるいは電子ディジタル・コンテンツ・ストア１０３は、その顧客サービス・サポートをクリアリング・ハウス１０５に外注することもできる。

【００４０】３．中間市場パートナ（図示せず）

代替実施形態では、セキュア・ディジタル・コンテンツ

電子配布システム１００を使用して、中間市場パートナと呼ばれる他のビジネスにコンテンツ１１３を確実に提供することができる。このようなパートナとしては、コンテンツ１１３を配布するテレビ局またはビデオ・クラブ、ラジオ放送局またはレコード・クラブなど、非電子サービスを提供するディジタル・コンテンツ関連会社を含むことができる。また、このようなパートナとしては、レコード・スタジオ、複製業者、生産者など、録音の作成またはマーケティングの一部として素材を扱う他の信頼できる当事者も含むことができる。このような中間市場パートナは、コンテンツ１１３を暗号化解除するために、クリアリング・ハウス１０５からのクリアランスが必要である。

【００４１】４．クリアリング・ハウス１０５

クリアリング・ハウス１０５は、ＳＣ内に暗号化されたコンテンツ１１３の販売または許可された使用あるいはその両方に関連するすべてのトランザクションに関するライセンス許可および記録保持を行う。クリアリング・ハウス１０５がコンテンツ１１３用の暗号化解除キーを求める要求を中間ユーザまたはエンドユーザから受け取ると、クリアリング・ハウス１０５は、要求内の情報の完全性および信憑性を妥当性検査し、その要求が電子ディジタル・コンテンツ・ストアまたはコンテンツ・プロバイダ１０１によって許可されたことを検証し、要求された使用がコンテンツ・プロバイダ１０１によって定義されたコンテンツ使用条件に適合することを検証する。このような検証が履行されると、クリアリング・ハウス１０５はライセンスＳＣにパックしたコンテンツ１１３用の暗号化解除キーを要求側エンドユーザに送信する。このキーは、許可ユーザだけがそれを検索できるように暗号化される。エンドユーザの要求が検証不能であるか、不完全であるか、または許可されていない場合、クリアリング・ハウス１０５は暗号化解除キーを求めるその要求を拒絶する。

【００４２】クリアリング・ハウス１０５は、すべてのトランザクションを記録し、即時、定期的、または制限付きで電子ディジタル・コンテンツ・ストア１０３およびコンテンツ・プロバイダ１０１などの担当当事者にそれを報告することができる。この報告は、それによりコンテンツ・プロバイダ１０１にコンテンツ１１３の販売を通知することができ、電子ディジタル・コンテンツ・ストア１０３がその顧客への電子送達の監査証跡を入手することができる手段である。また、クリアリング・ハウス１０５は、ＳＣ内の情報が損なわれているかまたはコンテンツの使用条件に適合しないことを検出した場合、コンテンツ・プロバイダ１０１または電子ディジタル・コンテンツ・ストア１０３あるいはその両方に通知することもできる。クリアリング・ハウス１０５のデータベースのトランザクション記録リポジトリ機能は、データ・マイニングまたは報告書作成用に構造化されている。

【００４３】他の実施形態では、クリアリング・ハウス１０５は、償還、伝送障害、購入紛争など、トランザクションに関する顧客サポートおよび例外処理を行うことができる。クリアリング・ハウス１０５は、権利管理および計量のための信頼できる管理人を提供する独立エンティティとして運営することができる。これは、必要に応じて請求および決済を行う。電子クリアリング・ハウスの例としては、Secure-Bank.comと、ビザ／マスター・カードによるセキュア・エレクトロニック・トランザクション（ＳＥＴ）を含む。一実施形態のクリアリング・ハウス１０５はエンドユーザ装置１０９にとってアクセス可能なウェブ・サイトである。他の実施形態のクリアリング・ハウス１０５は電子ディジタル・コンテンツ・ストア１０３の一部である。

【００４４】５．エンドユーザ装置１０９

エンドユーザ装置１０９は、セキュア・ディジタル・コンテンツ電子配布システム１００の仕様に適合するエンドユーザ・プレーヤ・アプリケーション１９５（後述する）を含む任意のプレーヤ装置にすることができる。このような装置としては、ＰＣ、セット・トップ・ボックス（ＩＲＤ）、インターネット家電を含むことができる。エンドユーザ・プレーヤ・アプリケーション１９５は、ソフトウェアまたは消費者エレクトロニクス・ハードウェアあるいはその両方で実現することができるだろう。再生、記録、ライブラリ管理の諸機能に加え、エンドユーザ・プレーヤ・アプリケーション１９５は、エンドユーザ装置１０９で権利管理を可能にするためのＳＣ処理を行う。エンドユーザ装置１０９は、ディジタル・コンテンツを含むＳＣのダウンロードおよび記憶を管理し、クリアリング・ハウス１０５から暗号化ディジタル・コンテンツ・キーの受取りを要求して管理し、ディジタル・コンテンツをコピーまたは再生するたびにウォータマークを処理し、ディジタル・コンテンツの使用条件に応じて作成したコピー数（またはコピーの削除）を管理し、許されるならば外部媒体または携帯用消費者装置へのコピーを実行する。携帯用消費者装置は、ウォータマークに埋め込まれたコンテンツの使用条件を処理するために、エンドユーザ・プレーヤ・アプリケーション１９５の諸機能のサブセットを実行することができる。エンドユーザおよびエンドユーザ・プレーヤ・アプリケーション１９５という用語は、これを通して、その使用またはエンドユーザ装置１０９上での実行を通して意味するために使用する。

【００４５】６．伝送インフラストラクチャ１０７

セキュア・ディジタル・コンテンツ電子配布システム１００は、電子ディジタル・コンテンツ・ストア１０３とエンドユーザ装置１０９とを接続する伝送ネットワークとは無関係のものである。これは、インターネットなどのポイントツーポイント配布モデルと、ディジタル同報

通信テレビなどの同報通信配布モデルの両方をサポートする。

【００４６】同じツールおよびアプリケーションを使用して様々な伝送インフラストラクチャ１０７によりコンテンツ１１３のトランザクションを取得し、パッケージ化し、追跡する場合でも、顧客にサービスを送達する際のプレゼンテーションおよび方法は、選択したインフラストラクチャおよび配布モデルに応じて様々になる可能性がある。また、低帯域インフラストラクチャより高帯域インフラストラクチャの方がより容認できる応答時間で高品質のディジタル・コンテンツを送達できるので、転送中のコンテンツ１１３の品質も様々になる可能性がある。ポイントツーポイント配布モデル用に設計されたサービス・アプリケーションは、同報通信配布モデルもサポートするように適合させることができる。

【００４７】Ｃ．システム用途

セキュア・ディジタル・コンテンツ電子配布システム１００により、諸費者またはビジネスのいずれであっても、エンドユーザ装置１０９にコンテンツ１１３の高品質な電子コピーを確実に送達することができ、コンテンツ１１３の使用を規制し追跡することができる。

【００４８】セキュア・ディジタル・コンテンツ電子配布システム１００は、新しい流通経路と既存の流通経路をともに使用して、様々な消費者サービスおよびビジネス間サービスに配備することができるだろう。特定の各サービスは、セキュア・ディジタル・コンテンツ電子配布システム１００の権利管理機能により実施可能な異なる金融モデルを使用することができるだろう。卸売りまたは小売り用の購入、ペイパーリッスン使用、加入サービス、コピー／コピー禁止制限、または再配布などのモデルは、クリアリング・ハウス１０５の権利管理とエンドユーザ・プレーヤ・アプリケーション１９５のコピー保護機能により実現することができるだろう。

【００４９】セキュア・ディジタル・コンテンツ電子配布システム１００により、電子ディジタル・コンテンツ・ストア１０３および中間市場パートナには、コンテンツ１１３を販売するサービスを作成する際に多大な柔軟性が与えられる。同時に、このシステムは、コンテンツ・プロバイダ１０１に対し、コンテンツ１１３のライセンスに対する適切な補償が受けられるようにそのディジタル資産が保護され計量されるという一定のレベルの保証を提供する。

【００５０】II．暗号概念およびセキュア・ディジタル・コンテンツ電子配布システムへの応用

セキュア・ディジタル・コンテンツ電子配布システム１００内のライセンス制御は暗号の使用に基づくものである。この項では、本発明の基本的な暗号技術を紹介する。公開キー暗号化、対称キー暗号化、ディジタル・シグニチャ、ディジタル・ウォータマーク、ディジタル証書の使用が知られている。

【００５１】Ａ．対称アルゴリズム

セキュア・ディジタル・コンテンツ電子配布システム１００では、コンテンツ・プロバイダ１０１は、対称アルゴリズムを使用してコンテンツを暗号化する。同じキーを使用してデータを暗号化し、暗号化解除するので、このアルゴリズムは対称アルゴリズムと呼ばれる。データ送信側とメッセージ受信側はこのキーを共用しなければならない。共用キーはここでは対称キーという。セキュア・ディジタル・コンテンツ電子配布システム１００のアーキテクチャは、特定の実施用に選択した特定の対象アルゴリズムとは無関係のものである。

【００５２】一般的な対称アルゴリズムは、ＤＥＳ、ＲＣ２、ＲＣ４である。ＤＥＳとＲＣ２はどちらもブロック暗号である。ブロック暗号は、一度に１ブロック分のデータ・ビットを使用してデータを暗号化する。ＤＥＳは、公式の米国政府暗号化規格であり、６４ビットのブロック・サイズを有し、５６ビットのキーを使用する。トリプルＤＥＳは、単純なＤＥＳによって達成されるセキュリティを増加するために一般に使用されている。ＲＣ２は、ＲＳＡデータ・セキュリティによって設計されたものである。ＲＣ２は、可変キーサイズ暗号を使用し、６４ビットのブロック・サイズを有する。同じくＲＳＡデータ・セキュリティによって設計されたＲＣ４は、可変キーサイズ・ストリーム暗号である。ストリーム暗号は、一度に単一データ・ビットを操作する。ＲＳＡデータ・セキュリティでは、ＲＣ４の場合、出力バイトあたり８～１６回のマシン操作が必要であると主張している。

【００５３】ＩＢＭでは、ＳＥＡＬという高速アルゴリズムを設計した。ＳＥＡＬは、可変長キーを使用し、３２ビット・プロセッサ用に最適化されたストリーム・アルゴリズムである。ＳＥＡＬでは、データ・バイトあたり約５つの基本的なマシン命令を必要とする。使用した１６０ビット・キーがすでに前処理されて内部テーブル内に入っている場合、５０ＭＨｚで４８６ベースのコンピュータは７．２メガバイト／秒でＳＥＡＬコードを実行する。

【００５４】マイクロソフトでは、同社のCryptoAPIの概要に関する文書で暗号化性能ベンチマークの結果を報告している。この結果は、Windows NT 4.0を搭載した１２０ＭＨｚのペンティアムベースのコンピュータ上でマイクロソフトのCryptoAPIを使用するアプリケーションを実行することによって得られたものである。

【００５５】

【表１】

暗号	キー・サイズ	キー・セットアップ時間	暗号化速度
DES	56	460	1,138,519
RC2	40	40	286,888
RC4	40	151	2,377,723

【００５６】Ｂ．公開キー・アルゴリズム
セキュア・ディジタル・コンテンツ電子配布システム１００では、公開キーを使用して対称キーおよびその他の小さいデータ・ピースを暗号化する。公開キー・アルゴリズムでは、２つのキーを使用する。この２つのキーは、一方のキーで暗号化したデータがもう一方のキーのみによって暗号化解除できるように数学的に関連付けられている。これらのキーのオーナは、一方のキーを秘密（秘密キー）に保ち、第２のキー（公開キー）を公に配布する。
【００５７】公開キー・アルゴリズムを使用した機密メッセージの伝送を確保するために、受信側の公開キーを使用してメッセージを暗号化しなければならない。関連の秘密キーを有する受信側だけがそのメッセージを暗号化解除することができる。また、公開キー・アルゴリズムは、ディジタル・シグニチャを生成するためにも使用する。秘密キーはその目的に使用する。以下の項ではディジタル・シグニチャに関する情報を示す。
【００５８】最も一般的に使用する公開キー・アルゴリズムは、ＲＳＡ公開キー暗号である。これは、業界では事実上の公開キー標準になっている。同じく暗号化およびディジタル・シグニチャのために十分機能する他のアルゴリズムとしては、ElGamalとRabinがある。ＲＳＡは可変キー長暗号である。
【００５９】対称キー・アルゴリズムは公開キー・アルゴリズムよりかなり高速である。ソフトウェアでは、一般にＤＥＳはＲＳＡの少なくとも１００倍の速度である。このため、ＲＳＡはバルク・データの暗号化に使用しない。ＲＳＡデータ・セキュリティは、９０ＭＨｚのペンティアム・マシンではＲＳＡデータ・セキュリティのツールキットＢＳＡＦＥ３．０の秘密キー動作（秘密キーを使用する暗号化または暗号化解除）のスループットが５１２ビット・モジュールでは２１．６キロビット／秒になり、１０２４ビット・モジュールでは７．４キロビット／秒になると報告している。
【００６０】Ｃ．ディジタル・シグニチャ
セキュア・ディジタル・コンテンツ電子配布システム１００では、ＳＣの発行者は、ディジタル方式でそれにサインすることによりＳＣの完全性を保護する。一般に、あるメッセージのディジタル・シグニチャを作成するために、メッセージ・オーナはまずメッセージ・ダイジェスト（以下に定義する）を計算し、次にオーナの秘密キーを使用してそのメッセージ・ダイジェストを暗号化する。メッセージはそのシグニチャとともに配布される。メッセージの受信側は、まずメッセージ・オーナの公開キーを使用してシグニチャを暗号化解除してメッセージ・ダイジェストを回復することにより、ディジタル・シグニチャを検証することができる。次に、受信側は、受信したメッセージのダイジェストを計算し、そのダイジェストと回復したダイジェストとを比較する。配布中にメッセージが変更されていない場合、計算したダイジェストと回復したダイジェストは等しくなければならない。
【００６１】セキュア・ディジタル・コンテンツ電子配布システム１００では、ＳＣは複数のデータ・パーツを含むので、各パーツごとにダイジェストが計算され、連結したパーツ・ダイジェストについて要約ダイジェストが計算される。要約ダイジェストは、ＳＣの発行者の秘密キーを使用して暗号化される。暗号化要約ダイジェストは、ＳＣ用の発行者のディジタル・シグニチャになる。パーツ・ダイジェストとディジタル・シグニチャはＳＣの本体に含まれる。ＳＣの受信側は、受信したディジタル・シグニチャとパーツ・ダイジェストにより、ＳＣとそのパーツの完全性を検証することができる。
【００６２】メッセージ・ダイジェストを計算するために一方向ハッシュ・アルゴリズムを使用する。ハッシュ・アルゴリズムは、可変長入力メッセージを取得し、それを固定長ストリングであるメッセージ・ダイジェストに変換する。一方向ハッシュ・アルゴリズムは、１つの方向でのみ動作する。すなわち、入力メッセージ用のダイジェストを計算することは容易であるが、そのダイジェストから入力メッセージを生成することは非常に困難（計算上、実行不可能）である。一方向ハッシュ関数の特性により、メッセージ・ダイジェストをそのメッセージのフィンガプリントと見なすことができる。
【００６３】より一般的な一方向ハッシュ関数は、ＲＳＡデータ・セキュリティによるＭＤ５と、米国National Institute of Technology and Standards（ＮＩＴＳ）によって設計されたＳＨＡである。
【００６４】Ｄ．ディジタル証書
ディジタル証書は、ディジタル方式でサインしたメッセージを送信した人物またはエンティティのアイデンティティを立証または検証するために使用する。証書は、公開キーをある人物またはエンティティにバインドする、証明機関によって発行されたディジタル文書である。この証書は、公開キー、人物またはエンティティの名前、満了日、証明機関の名称、その他の情報を含む。また、証書は、証明機関のディジタル・シグニチャも含む。

【００６５】あるエンティティ（または人物）がその公開キーでサインし、そのディジタル証書を添付したメッセージを送信すると、そのメッセージの受信側は証書からそのエンティティの名前を使用して、そのメッセージを受け入れるかどうかを判断する。

【００６６】セキュア・ディジタル・コンテンツ電子配布システム１００では、エンドユーザ装置１０９が発行したものを除くすべてのＳＣは、そのＳＣの作成者の証書を含む。エンドユーザ装置１０９はそのＳＣ内に証書を含む必要はない。というのは、多くのエンドユーザは非真正証明機関によって発行された証書を取得するかまたは証書を有する必要がないからである。セキュア・ディジタル・コンテンツ電子配布システム１００のクリアリング・ハウス１０５は、電子ディジタル・コンテンツ・ストア１０３に証書を発行する選択権を有する。このため、エンドユーザ装置１０９は、電子ディジタル・コンテンツ・ストア１０３がセキュア・ディジタル・コンテンツ電子配布システム１００によって許可されていることを独立して検証することができる。

【００６７】Ｅ．ＳＣ図形表現のガイド

本書では、ＳＣを図形表現するために、暗号化パーツ、非暗号化パーツ、暗号化キー、証書を示す図面を使用する。次に図５を参照すると、同図はＳＣ２００の図面例である。ＳＣの図では以下の記号を使用する。キー２０１は公開キーまたは秘密キーである。キーの歯はキー・オーナを示し、たとえば、クリアリングハウスの場合はＣＬＲＮＧＨである。ハンドル内部のＰＢはそれが公開キーであることを示し、したがって、キー２０１はクリアリングハウスの公開キーである。ハンドル内部のＰＶはそれが秘密キーであることを示す。菱形はエンドユーザ・ディジタル・シグニチャ２０２である。頭文字はどの秘密キーを使用してそのシグニチャを作成したかを示し、したがって、ＥＵは以下の表によればエンドユーザのディジタル・シグニチャである。対称キー２０３はコンテンツを暗号化するために使用する。暗号化対称キー・オブジェクト２０４は、ＣＬＲＮＧＨのＰＢで暗号化した対称キー２０３を含む。その長方形の上縁にあるキーはそのオブジェクトの暗号化で使用するキーである。長方形内部の記号またはテキストは、暗号化オブジェクト（この場合は対称キー）を示す。この例ではトランザクションＩＤ暗号化オブジェクト２０５である、もう１つの暗号化オブジェクトを示す。また、コンテンツ・ライセンス管理用の使用条件２０６は以下に記載する通りである。ＳＣ２００は、使用条件２０６と、トランザクションＩＤ暗号化オブジェクト２０５と、アプリケーションＩＤ暗号化オブジェクト２０７と、暗号化対称キー・オブジェクト２０４とを含み、いずれもエンドユーザ・ディジタル・シグニチャ２０２でサインされている。

【００６８】以下の表は、ＳＣの署名者を識別する頭文字を示している。

【００６９】

【表２】

頭文字	コンポーネント
CP	コンテンツ・プロバイダ101
MS	電子ディジタル・コンテンツ・ストア103
HS	コンテンツ・ホスト・サイト111
EU	エンドユーザ装置109
CH	クリアリング・ハウス105
CA	証明機関（図示せず）

【００７０】Ｆ．セキュア・コンテナ暗号化の例

以下の表および図は、ＳＣからの情報を作成し回復するために使用する暗号化および暗号化解除プロセスの概要を示す。このプロセス概要で作成され暗号化解除されるＳＣは一般的なＳＣである。これは、セキュア・ディジタル・コンテンツ電子配布システム１００における権利管理に使用する特定のＳＣタイプのいずれかを表すものではない。このプロセスは、暗号化プロセスについて図６に記載した諸ステップからなるものである。

【００７１】図６の暗号化プロセスのプロセス・フロープロセス

３０１　送信側はランダムな対称キーを生成し、それを使用してコンテンツを暗号化する。

３０２　送信側はハッシュ・アルゴリズムにより暗号化コンテンツを実行して、コンテンツ・ダイジェストを生成する。

３０３　送信側は受信側の公開キーを使用して対称キーを暗号化する。ＰＢＲＥＣＰＮＴは受信側の公開キーを意味する。

３０４　送信側はステップ３０２で使用したのと同じハッシュ・アルゴリズムにより暗号化対称キーを実行して、対称キー・ダイジェストを生成する。

３０５　送信側はステップ３０２で使用したのと同じハッシュ・アルゴリズムによりコンテンツ・ダイジェストと対称キー・ダイジェストの連結を実行して、ＳＣダイジェストを生成する。

３０６　送信側は送信側の秘密キーでＳＣダイジェストを暗号化して、ＳＣ用のディジタル・シグニチャを生成する。ＰＶ　ＳＥＮＤＥＲは送信側の秘密キーを意味する。

３０７Ｂ　送信側は、暗号化コンテンツ、暗号化対称キー、コンテンツ・ダイジェスト、対称キー・ダイジェスト、送信側の証書、ＳＣシグニチャを含むＳＣファイルを作成する。

３０７Ａ　送信側は安全な通信を開始する前に証明機関から証書を入手していなければならない。証明機関は、送信側の公開キーと、送信側の名前をその証書に含め、それにサインする。ＰＶ　ＣＡＵＴＨＲは証明機関の秘密キーを意味する。送信側は受信側にＳＣを伝送する。

【００７２】図７の暗号化解除プロセスのプロセス・フロー

プロセス

４０８　受信側はＳＣを受信し、そのパーツを分解する。

４０９　受信側は、証明機関の公開キーでそれを暗号化解除することにより、送信側の証書内のディジタル・シグニチャを検証する。証書のディジタル・シグニチャが有効である場合、受信側は証書から送信側の公開キーを取得する。

４１０　受信側は送信側の公開キーを使用してＳＣのディジタル・シグニチャを暗号化解除する。これでＳＣダイジェストを回復する。ＰＢ　ＳＥＮＤＥＲは送信側の公開キーを意味する。

４１１　受信側は送信側が使用したのと同じハッシュ・アルゴリズムにより受信コンテンツ・ダイジェストと暗号化キー・ダイジェストの連結を実行して、ＳＣダイジェストを計算する。

４１２　受信側は、計算したＳＣダイジェストと送信側のディジタル・シグニチャにより回復したダイジェストとを比較する。両者が同じである場合、受信側は、受信ダイジェストが変更されていないことを確認し、暗号化解除プロセスを続行する。両者が同じではない場合、受信側はそのＳＣを破棄し、送信側に通知する。

４１３　受信側はステップ４１１で使用したのと同じハッシュ・アルゴリズムにより暗号化対称キーを実行して、対称キー・ダイジェストを計算する。

４１４　受信側は、計算した対称キー・ダイジェストとＳＣで受信したダイジェストとを比較する。これが同じである場合、受信側は、暗号化対称キーが変更されていないことを把握する。受信側は暗号化解除プロセスを続行する。これが有効ではない場合、受信側はそのＳＣを破棄し、送信側に通知する。

４１５　受信側はステップ４１１で使用したのと同じハッシュ・アルゴリズムにより暗号化コンテンツを実行して、コンテンツ・ダイジェストを計算する。

４１６　受信側は、計算したコンテンツ・ダイジェストとＳＣで受信したダイジェストとを比較する。これが同じである場合、受信側は、暗号化コンテンツが変更されていないことを把握する。次に受信側は暗号化解除プロセスを続行する。これが有効ではない場合、受信側はそのＳＣを破棄し、送信側に通知する。

４１７　受信側は、受信側の秘密キーを使用して暗号化対称キーを暗号化解除する。これで対称キーを回復する。ＰＶ　ＲＥＣＰＮＴは受信側の秘密キーを意味する。

４１８　受信側は対称キーを使用した暗号化コンテンツを暗号化解除する。これでコンテンツを回復する。

【００７３】III. セキュア・ディジタル・コンテンツ電子配布システムのフロー

セキュア・ディジタル・コンテンツ電子配布システム１００は、システムの様々な関係者が使用する複数のコンポーネントからなるものである。このような関係者としては、コンテンツ・プロバイダ１０１、電子ディジタル・コンテンツ・ストア１０３、エンドユーザ装置１０９によるエンドユーザ、クリアリング・ハウス１０５を含む。セキュア・ディジタル・コンテンツ電子配布システム１００の概要として高レベル・システム・フローを使用する。以下に概略を示すこのフローは、システム１００全体を通過するコンテンツを追跡する。そのうえ、このフローは、コンテンツ１１３の購入、ロック解除、使用のためのトランザクションを実行するために関係者が使用する諸ステップの概略を示す。このシステム・フローで行う想定の一部としては以下のものを含む。

・　これは、ディジタル・コンテンツ・サービス（ＰＣへのポイントツーポイント・インタフェース）用のシステム・フローである。

・　コンテンツ・プロバイダ１０１は、（音楽オーディオ例として）ＰＣＭ未圧縮フォーマットでオーディオ・ディジタル・コンテンツを提示する。

・　コンテンツ・プロバイダ１０１はＯＤＢＣ適合データベース内にメタデータを有するか、あるいはコンテンツ・プロバイダ１０１はコンテンツ情報処理サブシステム内にデータを直接入力するかまたは規定のＡＳＣＩＩファイル・フォーマットでデータをすでに提供していることになる。

・　金融上の決済は電子ディジタル・コンテンツ・ストアによって行われる。

・　コンテンツ１１３は単一コンテンツ・ホスト・サイト１１１でホストとして処理される。

【００７４】当業者であれば、これらの想定は、同報通信されるディジタル・コンテンツ、たとえば、音楽、ビデオ、プログラムならびに電子配布システムの正確な性質に対処するように変更することができることに留意されたい。

【００７５】以下のプロセス・フローは図１ないし図４に示されている。

プロセス

１２１　未圧縮ＰＣＭオーディオ・ファイルはコンテンツ・プロバイダ１０１によってコンテンツ１１３として提供される。そのファイル名は、コンテンツ１１３用

のコンテンツ・プロバイダ１０１の固有の識別子とともにワーク・フロー・マネージャ１５４ツール内に入力される。

１２２　メタデータは、コンテンツ１１３用のコンテンツ・プロバイダ１０１の固有の識別子とデータベース・マッピング・テンプレートによって提供される情報を使用して、コンテンツ情報処理サブシステムによってコンテンツ・プロバイダのデータベース１６０から取り込まれる。

１２３　ワーク・フロー・マネージャ・ツール１５４は、コンテンツ・プロバイダ１０１での収集作成プロセスによりコンテンツ・フローを指示するために使用する。また、これは、任意の時点でシステム内のコンテンツ・ピースの状況を追跡するために使用することもできる。

１２４　コンテンツ１１３用の使用条件はコンテンツ情報処理サブシステム内に入力されるが、これは手動または自動のいずれでも行うことができる。このデータは、コピー制限規則と、必要と見なされたその他のビジネス規則を含む。メタデータの入力はすべて、そのデータのオーディオ処理と並行して行うことができる。

１２５　ウォータマーク・ツールは、コンテンツを識別するためにコンテンツ・プロバイダ１０１が必要と見なすデータをコンテンツ１１３内に隠すために使用する。これは、それがいつ取り込まれたか、それがどこから来たか（この場合はコンテンツ・プロバイダ１０１）と、コンテンツ・プロバイダ１０１によって指定されたその他の情報を含むことができるだろう。

・　コンテンツ処理ツール１２５は、サポートされる様々な圧縮レベルの必要に応じて、コンテンツ１１３への等化、強弱の変化の調節、再サンプリングを実行する。

・　コンテンツ１１３は、コンテンツ処理ツール１２５を使用して所望の圧縮レベルまで圧縮される。次にコンテンツ１１３を再生して、この圧縮によって必要なレベルのコンテンツ１１３品質が得られることを検証することができる。必要であれば、等化、強弱の変化の調節、圧縮、再生品質チェックを所望な回数だけ実行することができる。

・　コンテンツ１１３とそのメタデータのサブセットは、ＳＣパッカによって対称キーで暗号化される。次にこのツールは、クリアリング・ハウス１０５の公開キーを使用してそのキーを暗号化し、暗号化対称キーを生成する。それを暗号化解除できるエンティティはクリアリング・ハウス１０５だけなので、このキーはコンテンツ１１３のセキュリティを損なわずにどこにでも伝送することができる。

１２６　次に、暗号化対称キー、メタデータ、コンテンツ１１３に関するその他の情報はＳＣパッカ・ツール１５２によってメタデータＳＣ内にパックされる。

１２７　次に、暗号化コンテンツ１１３とメタデータはコンテンツＳＣ内にパックされる。この時点で、コンテンツ１１３とメタデータに関する処理は完了する。

１２８　次に、メタデータＳＣは、コンテンツ分配ツール（図示せず）を使用してコンテンツ・プロモーション・ウェブ・サイト１５６に送られる。

１２９　コンテンツ分配ツールはコンテンツＳＣをコンテンツ・ホスト・サイト１１１に送る。コンテンツ・ホスト・サイトは、コンテンツ・プロバイダ１０１、クリアリング・ハウス１０５、またはコンテンツ・ホスト専用の特別な位置に存在することができる。このサイト用のＵＲＬは、メタデータＳＣに追加されたメタデータの一部である。

１３０　コンテンツ・プロモーション・ウェブ・サイト１５６は、システム１００に追加された新しいコンテンツ１１３を電子ディジタル・コンテンツ・ストア１０３に通知する。

１３１　コンテンツ収集ツールを使用して、電子ディジタル・コンテンツ・ストア１０３は次に、それらが販売したいと希望するコンテンツ１１３に対応するメタデータＳＣをダウンロードする。

１３２　電子ディジタル・コンテンツ・ストア１０３は、コンテンツ収集ツールを使用して、自分のウェブ・サイト上でコンテンツ１１３をプロモートするために使用したいと希望する任意のデータをメタデータＳＣから引き出すことになる。このメタデータの各部分へのアクセスは、所望であれば保護し支払い請求することができる。

１３３　この電子ディジタル・コンテンツ・ストア１０３に固有のコンテンツ１１３用の使用条件は、コンテンツ収集ツールを使用して入力される。このような使用条件としては、コンテンツ１１３の様々な圧縮レベルに応じた小売価格、コピー／再生制限を含む。

１３４　電子ディジタル・コンテンツ・ストア１０３固有の使用条件および元のメタデータＳＣは、ＳＣパッカ・ツールによってオファーＳＣ内にパックされる。

１３５　電子ディジタル・コンテンツ・ストア１０３のウェブ・サイトを更新した後、コンテンツ１１３はウェブをサーフィンしているエンドユーザに使用可能なものになる。

１３６　エンドユーザが購入したいと希望するコンテンツ１１３を見つけると、エンドユーザは音楽アイコンなどのコンテンツ・アイコンをクリックし、その項目は、電子ディジタル・コンテンツ・ストア１０３によって維持されているそのエンドユーザのショッピング・カートに追加される。エンドユーザはショッピングを完了すると、処理のために電子ディジタル・コンテンツ・ストア１０３に購入要求を提示する。

１３７　次に電子ディジタル・コンテンツ・ストア１０３は、クレジット・カード清算組織と対話して、現在ビジネスを行っているのと同じように資金を確保する。

１３８　　電子ディジタル・コンテンツ・ストア１０３はクレジット・カード清算組織からクレジット・カード認証番号を受け取ると、これをデータベース内に記憶し、ＳＣパッカ・ツールを呼び出してトランザクションＳＣを構築する。このトランザクションＳＣは、エンドユーザが購入したコンテンツ１１３用のオファーＳＣのすべてと、電子ディジタル・コンテンツ・ストア１０３まで追跡可能なトランザクションＩＤと、エンドユーザを識別する情報と、圧縮レベルと、使用条件と、購入した歌曲の価格リストを含む。

１３９　　次にこのトランザクションＳＣはエンドユーザ装置１０９に伝送される。

１４０　　トランザクションＳＣは、エンドユーザ装置１０９に到着すると、トランザクションＳＣをオープンし、エンドユーザの購入を承認するエンドユーザ・プレーヤ・アプリケーション１９５を開始する。次にエンドユーザ・プレーヤ・アプリケーション１９５は個々のオファーＳＣをオープンし、代替実施形態ではダウンロード時間の推定値をユーザに通知することができる。次にそのアプリケーションは、いつコンテンツ１１３をダウンロードしたいのかを指定するようユーザに要求する。

１４１　　エンドユーザがダウンロードを要求した時間に基づいて、エンドユーザ・プレーヤ・アプリケーション１９５はウェイクアップし、とりわけコンテンツ１１３用の暗号化対称キーと、トランザクションＩＤと、エンドユーザ情報とを含むオーダＳＣを構築することにより、ダウンロード・プロセスの始動を開始することになる。

１４２　　次にこのオーダＳＣは処理のためにクリアリング・ハウス１０５に送られる。

１４３　　クリアリング・ハウス１０５はオーダＳＣを受け取り、それをオープンし、いずれのデータも改竄されていないことを検証する。クリアリング・ハウス１０５は、エンドユーザによって購入された使用条件を妥当性検査する。このような使用条件は、コンテンツ・プロバイダ１０１によって指定されたものと適合しなければならない。この情報はデータベースにログインされる。

１４４　　すべてのチェックが完了すると、暗号化対称キーはクリアリング・ハウス１０５の秘密キーを使用して暗号化解除される。次に対称キーは、エンドユーザの公開キーを使用して暗号化される。この新しい暗号化対称キーは次にＳＣパッカによってライセンスＳＣ内にパッケージ化される。

１４５　　次にライセンスＳＣはエンドユーザに伝送される。

１４６　　ライセンスＳＣはエンドユーザ装置１０９側で受信されると、コンテンツＳＣがダウンロードされるまでメモリ内に記憶される。

１４７　　エンドユーザ装置１０９は、購入したコンテンツ１１３用の対応ライセンスＳＣを送信して、コンテンツ・ホスト設備１１１から要求する。

１４８　　コンテンツ１１３はエンドユーザ装置１０９に送られる。受信次第、コンテンツ１１３は対称キーを使用してエンドユーザ装置１０９によって暗号化解除される。

【００７６】IV. 権利管理アーキテクチャ・モデル

Ａ．アーキテクチャ層機能

図８は、セキュア・ディジタル・コンテンツ電子配布システム１００の権利管理アーキテクチャのブロック図である。アーキテクチャ上、ライセンス制御層５０１、コンテンツ識別層５０３、コンテンツ使用制御層５０５、コンテンツ・フォーマット層５０７という４つの層がセキュア・ディジタル・コンテンツ電子配布システム１００を表している。各層の全体的な機能目標と、各層の個々の重要機能について、この項で説明する。各層の機能は他の層の機能とはまったく無関係である。広範囲の制限内で各層の機能は、他の層の機能性に影響せずに同様の機能で代用することができる。明らかに、ある層からの出力は隣接層にとって容認できるフォーマットおよびセマンティクスを満足する必要がある。

【００７７】ライセンス制御層５０１は以下の点を保証するものである。

・　ディジタル・コンテンツは配布中に違法インターセプトおよび改竄から保護される。

・　コンテンツ１１３は正当なコンテンツ・オーナから発生し、ライセンス配布者、たとえば、電子ディジタル・コンテンツ・ストア１０３によって配布される。

・　ディジタル・コンテンツ購入者は適切にライセンスを受けたアプリケーションを有する。

・　配布者は、コンテンツ１１３のコピーが購入者またはエンドユーザに使用可能なものになる前に、購入者から支払を受ける。

・　報告のためにトランザクションの記録が保持される。

【００７８】コンテンツ識別層５０３は、著作権およびコンテンツ購入者のアイデンティティの検証を可能にするものである。コンテンツの著作権情報およびコンテンツ購入者のアイデンティティにより、認可されているか否かにかかわらず、コンテンツ１１３のすべてのコピーのソース追跡が可能になる。したがって、コンテンツ識別層５０３は著作権侵害と闘うための手段を提供する。

【００７９】コンテンツ使用制御層５０５は、コンテンツ１１３のコピーがストア使用条件５１９に応じて購入者の装置内で使用されることを保証するものである。ストア使用条件５１９は、コンテンツ１１３について許される再生回数およびローカル・コピー数と、コンテンツ１１３を外部携帯用装置に記録可能であるかどうかを指定することができる。コンテンツ使用制御層５０５内の諸機能は、コンテンツのコピー／再生使用を追跡し、コピー／再生状況を更新する。

【００８０】コンテンツ・フォーマット層５０７は、コンテンツ・オーナの設備内でのその固有表現からセキュア・ディジタル・コンテンツ電子配布システム１００のサービス機能および配布手段に適合する形式へのコンテンツ１１３のフォーマット変換を可能にするものである。この変換処理は、圧縮コード化と、周波数等化および振幅ダイナミック調整など、それに関連する前処理とを含むことができる。コンテンツ１１３がオーディオである場合、購入者側では、再生または携帯用装置への転送に適したフォーマットを達成するように受信したコンテンツ１１３を処理する必要もある。

【００８１】Ｂ．機能区分およびフロー

権利管理アーキテクチャ・モデルを図８に示すが、これはセキュア・ディジタル・コンテンツ電子配布システム１００を構成する動作コンポーネントに対するアーキテクチャ層のマッピングと、各層の重要機能を示している。

【００８２】１．コンテンツ・フォーマット層５０７

コンテンツ・フォーマット層５０７に関連する一般的な機能は、コンテンツ・プロバイダ１０１でのコンテンツ前処理５０２および圧縮５１１と、エンドユーザ装置１０９でのコンテンツ・スクランブル解除５１３および圧縮解除５１５である。前処理の必要性と特定の機能の例については前述した通りである。コンテンツ圧縮５１１は、コンテンツ１１３のファイル・サイズとその伝送時間を低減するために使用する。セキュア・ディジタル・コンテンツ電子配布システム１００では、コンテンツ１１３および伝送媒体のタイプに適した任意の圧縮アルゴリズムを使用することができる。音楽の場合、ＭＰＥＧ１／２／４、ドルビーＡＣ－２およびＡＣ－３、ソニー適応変換コーディング（ＡＴＲＡＣ）、低ビット伝送速度アルゴリズムは、通常使用される圧縮アルゴリズムの一部である。コンテンツ１１３は、必要な記憶サイズを低減するために圧縮した形式でエンドユーザ装置１０９に記憶される。これは、アクティブ再生中に圧縮解除される。また、アクティブ再生中にはスクランブル解除も行われる。スクランブルの目的およびタイプについては、コンテンツ使用制御層５０５の説明時に後述する。

【００８３】２．コンテンツ使用制御層５０５

コンテンツ使用制御層５０５は、エンドユーザ装置１０９でのコンテンツ１１３の使用に課せられる条件または制限の指定および執行を可能にする。この条件は、コンテンツ１１３について許される再生回数、コンテンツ１１３の２次コピーが許されるかどうか、２次コピーの数、コンテンツ１１３を外部携帯用装置にコピー可能かどうかを指定することができる。コンテンツ・プロバイダ１０１は、許容できる使用条件５１７を設定し、それをＳＣに入れて電子ディジタル・コンテンツ・ストア１０３に伝送する（ライセンス制御層５０１の項を参照）。それによってコンテンツ・プロバイダ１０１が設定した元の条件が無効にならない限り、電子ディジタル・コンテンツ・ストア１０３は使用条件５１７を大きくするかまたは狭くすることができる。次に電子ディジタル・コンテンツ・ストア１０３はすべてのストア使用条件５１９を（ＳＣに入れて）エンドユーザ装置１０９およびクリアリング・ハウス１０５に伝送する。クリアリング・ハウス１０５は、エンドユーザ装置１０９へのコンテンツ１１３のリリースを許可する前に、使用条件妥当性検査５２１を実行する。

【００８４】コンテンツの使用条件５１７の執行は、エンドユーザ装置１０９内のコンテンツ使用制御層５０５によって実行される。第１に、コンテンツ１１３を受信すると、エンドユーザ装置１０９内のコンテンツ識別層５０３からのコピーは、初期コピー／再生許可を表すコピー／再生コード５２３でコンテンツ１１３にマークを付ける。第２に、プレーヤ・アプリケーション１９５は、それをエンドユーザ装置１０９に記憶する前にコンテンツ１１３に暗号法でスクランブルをかける。プレーヤ・アプリケーション１９５は各コンテンツ項目ごとにスクランブル・キーを生成し、そのキーは暗号化され、エンドユーザ装置１０９に隠される。次に、エンドユーザ１０９がコピーまたは再生のためにコンテンツ１１３にアクセスするたびに、エンドユーザ装置１０９は、コンテンツ１１３のスクランブル解除と再生またはコピーの実行を許可する前にコピー／再生コードを検証する。また、エンドユーザ装置１０９は、コンテンツ１１３のオリジナル・コピー内または新しい２次コピー上のコピー／再生コードを適切に更新する。コピー／再生コーディングは、圧縮されたコンテンツ１１３について実行される。すなわち、コピー／再生コードを埋め込む前にコンテンツ１１３を圧縮解除する必要はない。

【００８５】エンドユーザ装置１０９は、ライセンス・ウォータマーク５２７を使用してコンテンツ１１３内にコピー／再生コードを埋め込む。埋め込まれたデータを読み取ったり変更することができるのは、埋め込まれたアルゴリズムと関連のスクランブル・キーを良く知っているエンドユーザ・プレーヤ・アプリケーション１９５のみである。このデータは人間の監視者にとっては目に見えないかまたは聞こえないものであり、すなわち、このデータはコンテンツ１１３に対して感知できるほどの劣化をもたらすことはない。ウォータマークはコンテンツ処理、データ圧縮、Ｄ／Ａ変換およびＡ／Ｄ変換、通常のコンテンツ処理によってもたらされる信号劣化といういくつかのステップ後も存続するので、ウォータマークはアナログ表現を含む任意の表現形式でコンテンツ１１３とともに持続する。代替実施形態では、ライセンス・ウォータマーク５２７を使用してコピー／再生コードをコンテンツ１１３内に埋め込む代わりに、エンドユーザ・プレーヤ・アプリケーション１９５は確実に記憶した使用条件５１９を使用する。

【００８６】３．コンテンツ識別層５０３
コンテンツ識別層５０３の一部として、コンテンツ・プロバイダ１０１は、ライセンス・ウォータマーク５２７を使用して、コンテンツ識別子、コンテンツ・オーナなどのデータと、出版日、配布地域などのその他の情報をコンテンツ１１３に埋め込む。このウォータマークはここでは著作権ウォータマーク５２９という。受領すると、エンドユーザ装置１０９はコンテンツ１１３のコピーにコンテンツ購入者の名前とトランザクションＩＤ５３５（以下のライセンス制御層５０１の項を参照）、ならびにライセンス日や使用条件５１７などのその他の情報でウォータマークを付ける。このウォータマークはここではライセンス・ウォータマークという。承認された方法で入手しまたはそうではなく、コンテンツ品質を保存するオーディオ処理の対象となるコンテンツ１１３のいずれのコピーにも、著作権ウォータマークとライセンス・ウォータマークが付いている。コンテンツ識別層５０３は著作権侵害を阻止するものである。
【００８７】４．ライセンス制御層５０１
ライセンス制御層５０１は、無許可インターセプトからコンテンツ１１３を保護し、エンドユーザ装置１０９に適切にライセンスを与え、認可電子ディジタル・コンテンツ・ストア１０３とのライセンス購入トランザクションを正常に完了したエンドユーザに対してのみコンテンツが個別にリリースされることを保証する。ライセンス制御層５０１は二重暗号化５３１によってコンテンツ１１３を保護する。コンテンツ１１３はコンテンツ・プロバイダ１０１によって生成された暗号化対称キーを使用して暗号化され、その対称キーはクリアリング・ハウスの公開キー６２１を使用して暗号化される。最初に対称キーを回復できるのはクリアリング・ハウス１０５のみである。
【００８８】ライセンス制御は、「信頼できる当事者」としてクリアリング・ハウス１０５とともに設計されている。ライセンス要求５３７（すなわち、エンドユーザ装置１０９へのコンテンツ１１３用の対称キー６２３）に関する許可をリリースする前に、クリアリング・ハウス１０５は、トランザクション５４１とライセンス認可５４３が完全かつ真正であること、電子ディジタル・コンテンツ・ストア１０３が電子コンテンツ１１３の販売に関してセキュア・ディジタル・コンテンツ電子配布システム１００からの認可を得ていること、エンドユーザが適切にライセンスを受けたアプリケーションを有することを検証する。監査／報告５４５により、報告書を作成することができ、セキュア・ディジタル・コンテンツ電子配布システム１００内の他の認可当事者とライセンス・トランザクション情報を共用することができる。
【００８９】ライセンス制御はＳＣ処理５３３により実施される。ＳＣは、システム動作コンポーネント間で暗号化コンテンツ１１３と情報を配布するために使用する（詳細については以下のＳＣの詳細構造の項を参照）。ＳＣは、暗号化、ディジタル・シグニチャ、ディジタル証書を使用して電子情報またはコンテンツ１１３を無許可インターセプトおよび変更から保護する情報の暗号キャリアである。また、これは、電子データの信憑性検証も可能にする。
【００９０】ライセンス制御では、コンテンツ・プロバイダ１０１、電子ディジタル・コンテンツ・ストア１０３、クリアリング・ハウス１０５が、このようなコンポーネントを立証するために使用する、評判の良い証明機関からの真正の暗号ディジタル証書を有することが必要である。エンドユーザ装置１０９はディジタル証書を有する必要はない。
【００９１】Ｃ．コンテンツ配布ライセンス制御
図９は、図８のライセンス制御層に適用されたときのコンテンツ配布ライセンス制御の概要を示すブロック図である。同図では、電子ディジタル・コンテンツ・ストア１０３と、エンドユーザ装置１０９と、クリアリング・ハウス１０５がインターネットを介して相互接続され、これらのコンポーネント間でユニキャスト（ポイントツーポイント）伝送を使用することを示している。コンテンツ・プロバイダ１０１と電子ディジタル・コンテンツ・ストア１０３との通信も、インターネットまたはその他のネットワークによる可能性がある。エンドユーザ装置１０９と電子ディジタル・コンテンツ・ストア１０３とのコンテンツ購入商用トランザクションが標準のインターネット・ウェブ・プロトコルに基づくものであると想定する。ウェブベースの対話の一部として、エンドユーザは、購入するコンテンツ１１３を選択し、個人情報および金融情報を提供し、購入条件に同意する。電子ディジタル・コンテンツ・ストア１０３は、ＳＥＴなどのプロトコルを使用して取得機関から支払許可を得ることができるだろう。
【００９２】また、図９では、電子ディジタル・コンテンツ・ストア１０３がすでに標準のウェブ・プロトコルに基づいてエンドユーザ・プレーヤ・アプリケーション１９５をエンドユーザ装置１０９にダウンロードしたと想定する。このアーキテクチャでは、電子ディジタル・コンテンツ・ストア１０３はダウンロードしたプレーヤ・アプリケーション１９５に固有のアプリケーションＩＤを割り当て、後でアプリケーション・ライセンス検証を行うためにエンドユーザ装置１０９がそれを記憶しなければならない（以下参照）。
【００９３】全体的なライセンスの流れはコンテンツ・プロバイダ１０１から始まる。コンテンツ・プロバイダ１０１は、ローカルで生成した暗号化対称キーを使用してコンテンツ１１３を暗号化し、クリアリング・ハウス１０５の公開キー６２１を使用して対称キー６２３を暗号化する。代替実施形態の対称キーは、ローカルで生成する代わりに、クリアリング・ハウス１０５からコンテ

ンツ・プロバイダ１０１に送ることもできる。コンテンツ・プロバイダ１０１は、暗号化コンテンツ１１３の周りにコンテンツＳＣ６３０を作成し、暗号化対称キー６２３、ストア使用条件５１９、その他のコンテンツ１１３関連情報の周りにメタデータＳＣ６２０を作成する。すべてのコンテンツ１１３オブジェクトについて、１つのメタデータＳＣ６２０と１つのコンテンツＳＣ６３０が存在する。コンテンツ１１３オブジェクトは同一歌曲の圧縮レベルである場合もあれば、コンテンツ１１３オブジェクトはアルバム上の各歌曲である場合もあり、あるいはコンテンツ１１３オブジェクトはアルバム全体である場合もある。各コンテンツ１１３オブジェクトごとに、メタデータＳＣ６２０は、コンテンツ使用制御層５０５に関連するストア使用条件５１９も伝達する。

【００９４】コンテンツ・プロバイダ１０１は、１つまたは複数の電子ディジタル・コンテンツ・ストア１０３にメタデータＳＣ６２０を配布し（ステップ６０１）、１つまたは複数のコンテンツ・ホスト・サイトにコンテンツＳＣ６３０を配布する（ステップ６０２）。次に各電子ディジタル・コンテンツ・ストア１０３はオファーＳＣ６４１を作成する。オファーＳＣ６４１は通常、メタデータＳＣ６２０と同じ情報の多くを伝達し、コンテンツ・プロバイダ１０１のディジタル・シグニチャ６２４およびコンテンツ・プロバイダ１０１の証書（図示せず）を含む。前述のように、電子ディジタル・コンテンツ・ストア１０３は、初めにコンテンツ・プロバイダ１０１によって定義されたストア使用条件５１９（コンテンツ使用制御層が処理する）を大きくするかまたは狭くすることができる。任意選択で、コンテンツＳＣ６３０またはメタデータＳＣ６２０あるいはその両方には、コンテンツ・プロバイダ１０１のディジタル・シグニチャ６２４でサインする。

【００９５】エンドユーザ装置１０９と電子ディジタル・コンテンツ・ストア１０３とのコンテンツ購入トランザクション（ステップ６０３）の完了後、電子ディジタル・コンテンツ・ストア１０３はトランザクションＳＣ６４０を作成し、それをエンドユーザ装置１０９に転送する（ステップ６０４）。トランザクションＳＣ６４０は、固有のトランザクションＩＤ５３５と、購入者の名前（すなわち、エンドユーザの名前）（図示せず）と、エンドユーザ装置１０９の公開キー６６１と、購入したコンテンツ１１３に関連するオファーＳＣ６４１とを含む。図９のトランザクション・データ６４２はトランザクションＩＤ５３５とエンドユーザの名前（図示せず）の両方を表している。トランザクション・データ６４２は、クリアリング・ハウス１０５の公開キー６２１で暗号化される。任意選択で、トランザクションＳＣ６４０には、電子ディジタル・コンテンツ・ストア１０３のディジタル・シグニチャ６４３でサインする。

【００９６】トランザクションＳＣ６４０（およびそれに含まれるオファーＳＣ６４１）を受け取ると、エンドユーザ装置１０９上で実行されるエンドユーザ・プレーヤ・アプリケーション１９５はオーダＳＣ６５０によりクリアリング・ハウス１０５からライセンス認可を送信請求する。オーダＳＣ６５０は、オファーＳＣ６４１からの暗号化対称キー６２３およびストア使用条件５１９と、トランザクションＳＣ６４０からの暗号化トランザクション・データ６４２と、エンドユーザ装置１０９からの暗号化アプリケーションＩＤ５５１とを含む。代替実施形態のオーダＳＣ６５０には、エンドユーザ装置１０９のディジタル・シグニチャ６５２でサインする。

【００９７】エンドユーザ装置１０９からオーダＳＣ６５０を受け取ると、クリアリング・ハウス１０５は以下の点を検証する。

１．電子ディジタル・コンテンツ・ストア１０３がセキュア・ディジタル・コンテンツ電子配布システム１００から認可を得ている（クリアリング・ハウス１０５のデータベース１６０内に存在する）こと。

２．オーダＳＣ６５０が変更されていないこと。

３．トランザクション・データ６４２と対称キー６２３が完全かつ真正であること。

４．エンドユーザ装置１０９が購入した電子ストア使用条件５１９がコンテンツ・プロバイダ１０１が設定した使用条件５１７に適合していること。

５．アプリケーションＩＤ５５１が有効な構造を有し、それが認可電子ディジタル・コンテンツ・ストア１０３によって提供されたこと。

【００９８】この検証が成功した場合、クリアリング・ハウス１０５は、対称キー６２３とトランザクション・データ６４２を暗号化解除し、ライセンスＳＣ６６０を構築してエンドユーザ装置１０９に転送する（ステップ６０６）。ライセンスＳＣ６６０は対称キー６２３とトランザクション・データ６４２を伝達するが、いずれもエンドユーザ装置１０９の公開キー６６１を使用して暗号化されている。いずれかの検証が失敗した場合、クリアリング・ハウス１０５はエンドユーザ装置１０９へのライセンスを拒否し、エンドユーザ装置１０９に通知する。また、クリアリング・ハウス１０５は直ちに電子ディジタル・コンテンツ・ストア１０３にこの検証失敗を通知する。代替実施形態のクリアリング・ハウス１０５は、そのディジタル・シグニチャ６６３でライセンスＳＣ６６０にサインする。

【００９９】ライセンスＳＣ６６０を受け取った後、エンドユーザ装置１０９は、クリアリング・ハウス１０５から前に受け取った対称キー６２３およびトランザクション・データ６４２を暗号化解除し、コンテンツ・ホスト・サイト１１１からコンテンツＳＣ６３０を要求する（ステップ６０７）。コンテンツＳＣ６３０が到着すると（ステップ６０８）、エンドユーザ装置１０９は、対称キー６２３を使用してコンテンツ１１３を暗号化解除

し（ステップ６０９）、図８に関して前述したようにライセンス・ウォータマーク、コピー／再生コーディング、スクランブル、その他のコンテンツ１１３の処理のために、コンテンツ１１３およびトランザクション・データ６４２を他の層に渡す。

【０１００】最後に、クリアリング・ハウス１０５は、監査および追跡のために要約トランザクション報告をコンテンツ・プロバイダ１０１および電子ディジタル・コンテンツ・ストア１０３に定期的に伝送する（ステップ６１０）。

【０１０１】Ｖ．セキュア・コンテナ構造

Ａ．一般構造

セキュア・コンテナ（ＳＣ）は、相俟ってコンテンツ１１３のユニットまたはトランザクションの一部分を定義し、また使用条件、メタデータ、暗号化方法などの関連情報も定義する、複数のパーツからなる構造である。ＳＣは、情報の完全性、完璧さ、信憑性を検証できるように設計されている。ＳＣ内の情報の一部は、適正な許可を取得した後でなければアクセスできないように暗号化することができる。

【０１０２】ＳＣは、ＳＣとＳＣに含まれる各パーツに関する情報のレコードを有する少なくとも１つの素材一覧表（ＢＯＭ）パーツを含む。各パーツごとに、ＭＤ－５などのハッシュ・アルゴリズムを使用してメッセージ・ダイジェストが計算され、そのパーツ用のＢＯＭレコードに含まれる。各パーツのダイジェストはひとまとめに連結され、そのダイジェストからもう１つのダイジェストが計算され、ＳＣを作成するエンティティの秘密キーを使用して暗号化され、ディジタル・シグニチャを作成する。ＳＣを受け取る当事者は、そのディジタル・シグニチャを使用してすべてのダイジェストを検証し、ＳＣおよびそのすべてのパーツの完全性および完璧さを妥当性検査することができる。

【０１０３】以下の情報は、各パーツのレコードとともに、ＢＯＭ内のレコードとして含めることができる。どのレコードを含める必要があるかは、ＳＣのタイプによって決まる。

・　ＳＣのバージョン
・　ＳＣのＩＤ
・　ＳＣのタイプ（たとえば、オファー、オーダ、トランザクション、コンテンツ、メタデータ、プロモーション、ライセンス）
・　ＳＣの発行者
・　ＳＣが作成された日付
・　ＳＣの満了日
・　クリアリング・ハウスのＵＲＬ
・　含まれるパーツに使用するダイジェスト・アルゴリズムの記述（デフォルトはＭＤ－５）
・　ディジタル・シグニチャ暗号化に使用するアルゴリズムの記述（デフォルトはＲＳＡ）
・　ディジタル・シグニチャ（含まれるパーツの連結ダイジェストのすべての暗号化ダイジェスト）

【０１０４】ＳＣは複数のＢＯＭを含むことができる。たとえば、オファーＳＣ６４１は、そのＢＯＭを含む、元のメタデータＳＣ６２０の各パーツと、電子ディジタル・コンテンツ・ストア１０３によって追加された追加情報と、新しいＢＯＭからなる。メタデータＳＣ６２０のＢＯＭのレコードはオファーＳＣ６４１のＢＯＭに含まれる。このレコードは、その完全性を妥当性検査するために使用可能なメタデータＳＣ６２０のＢＯＭ用のダイジェストを含み、したがって、メタデータＳＣ６２０に含まれる各パーツの完全性もメタデータＳＣ６２０のＢＯＭに記憶されたパーツ・ダイジェスト値を使用して妥当性検査することができる。メタデータＳＣ６２０からのいずれのパーツも、オファーＳＣ６４１用に作成された新しいＢＯＭ内のレコードを有していない。電子ディジタル・コンテンツ・ストア１０３とメタデータＳＣ６２０のＢＯＭによって追加されたパーツのみが、新しいＢＯＭ内のレコードを有する。

【０１０５】ＳＣはキー記述パーツも含むことができる。キー記述パーツとしては、ＳＣ内の暗号化パーツに関する以下の情報を含むレコードを含むことができる。

・　暗号化パーツの名前
・　それが暗号化解除されたときにそのパーツのために使用する名前
・　そのパーツを暗号化するために使用する暗号化アルゴリズム
・　そのパーツを暗号化するために使用した公開暗号化キーを示すためのキー識別子または暗号化解除するときに暗号化パーツを暗号化解除するために使用する暗号化対称キー
・　対称キーを暗号化するために使用する暗号化アルゴリズム。このフィールドはキー記述パーツ内のレコードが暗号化パーツを暗号化するために使用した暗号化対称キーを含む場合のみ存在する。
・　対称キーを暗号化するために使用した公開暗号化キーのキー識別子。このフィールドはキー記述パーツ内のレコードが暗号化対称キーと、暗号化パーツを暗号化するために使用した対称キーの暗号化アルゴリズム識別子を含む場合のみ存在する。ＳＣが暗号化パーツを含まない場合、キー記述パーツは一切存在しない。

【０１０６】Ｂ．権利管理言語構文およびセマンティクス

権利管理言語は、コンテンツ１１３の購入後にエンドユーザによるコンテンツ１１３の使用に関する制限を定義するために値を割り当てることができるパラメータからなる。コンテンツ１１３の使用に関する制限は使用条件５１７である。各コンテンツ・プロバイダ１０１は、そのコンテンツ１１３の各項目ごとに使用条件５１７を指定する。電子ディジタル・コンテンツ・ストア１０３

は、メタデータＳＣ６２０内の使用条件５１７を解釈し、その情報を使用して、顧客に提示したい選択オプションを提供すると同時にコンテンツ１１３に関する小売購入情報を追加する。エンドユーザが購入のためにコンテンツ１１３の項目を選択した後、エンドユーザ装置１０９はストア使用条件５１９に基づいてコンテンツ１１３に関する許可を要求する。クリアリング・ハウス１０５がエンドユーザにラインセンスＳＣ６６０を送る前に、クリアリング・ハウス１０５は、要求したストア使用条件５１９がメタデータＳＣ６２０内にコンテンツ・プロバイダ１０１によって指定された許容できる使用条件５１７と一致していることを検証する。

【０１０７】エンドユーザ装置１０９が購入したコンテンツ１１３を受け取ると、ストア使用条件５１９はウォータマーク・ツールを使用してコンテンツ１１３内にコード化されるかまたは確実に記憶した使用条件５１９内にコード化される。エンドユーザ装置１０９上で実行されるエンドユーザ・プレーヤ・アプリケーション１９５は、コンテンツ１１３内にコード化されたストア使用条件５１９が執行されることを保証する。

【０１０８】コンテンツ１１３が音楽である実施形態の場合のストア使用条件５１９の例を以下に示す。

・　歌曲は記録可能である。
・　歌曲はｎ回再生可能である。

【０１０９】Ｃ．セキュア・コンテナのフローおよび処理の概要

メタデータＳＣ６２０は、コンテンツ・プロバイダ１０１によって構築され、歌曲などのコンテンツ１１３の項目を定義するために使用する。コンテンツ１１３のサイズは通常、電子ディジタル・コンテンツ・ストア１０３とエンドユーザが記述メタデータにアクセスするためにだけそのコンテナを効率よくダウンロードするには大きすぎるので、コンテンツ１１３自体はこのようなＳＣ内に含まれない。むしろ、ＳＣはコンテンツ１１３を指し示すための外部ＵＲＬ（ユニフォーム・リソース・ロケータ）を含む。また、ＳＣはコンテンツ１１３に関する記述情報と、歌曲コンテンツ１１３の場合は音楽用のＣＤカバー・アートまたはディジタル・オーディオ・クリップあるいはその両方などのその他の関連データを提供するメタデータも含む。

【０１１０】電子ディジタル・コンテンツ・ストア１０３は、それに関する認可を受けているメタデータＳＣ６２０をダウンロードし、オファーＳＣ６４１を構築する。要するに、オファーＳＣ６４１は、電子ディジタル・コンテンツ・ストア１０３が含めた追加情報とともにメタデータＳＣ６２０からの全パーツの一部とＢＯＭからなる。オファーＳＣ６４１が構築されると、オファーＳＣ６４１用の新しいＢＯＭが作成される。また、電子ディジタル・コンテンツ・ストア１０３は、エンドユーザが通常、コンテンツ１１３を購入できるように、それからメタデータ情報を抽出することにより、メタデータＳＣ６２０を使用して、エンドユーザにコンテンツ１１３の記述を提示するＨＴＭＬページをそのウェブ・サイト上に構築する。

【０１１１】電子ディジタル・コンテンツ・ストア１０３によって追加されるオファーＳＣ６４１内の情報は通常、メタデータＳＣ６２０に指定される使用条件５１７と、ストアのロゴのグラフィック画像ファイルやストアのウェブ・サイトへのＵＲＬなどのプロモーション・データの選択を狭くするためのものである。メタデータＳＣ６２０内のオファーＳＣ６４１のテンプレートは、オファーＳＣ６４１内で電子ディジタル・コンテンツ・ストア１０３がどの情報を指定変更できるか、電子ディジタル・コンテンツ・ストア１０３がどの追加情報を必要とするか、ならびに埋込みメタデータＳＣ６２０内にどのパーツが保持されるかを示す。

【０１１２】エンドユーザが電子ディジタル・コンテンツ・ストア１０３からコンテンツ１１３を購入することを決定すると、オファーＳＣ６４１がトランザクションＳＣ６４０に含まれる。電子ディジタル・コンテンツ・ストア１０３は、トランザクションＳＣ６４０を構築し、購入するコンテンツ１１３の各項目ごとにオファーＳＣ６４１を含め、それをエンドユーザ装置１０９に伝送する。エンドユーザ装置１０９は、トランザクションＳＣ６４０を受け取り、トランザクションＳＣ６４０と含まれるオファーＳＣ６４１の完全性を妥当性検査する。

【０１１３】オーダＳＣ６５０は、購入するコンテンツ１１３の各項目ごとにエンドユーザ装置１０９によって構築される。オファーＳＣ６４１からの情報と、トランザクションＳＣ６４０からの情報と、エンドユーザ装置１０９の構成ファイルからの情報が含まれる。オーダＳＣ６５０は一度に１つずつクリアリング・ハウス１０５に送られる。オーダＳＣ６５０がメタデータＳＣ６２０用のＢＯＭ内のレコードの１つとして含まれるクリアリング・ハウス１０５のＵＲＬも同じくオファーＳＣ６４１に含まれる。

【０１１４】クリアリング・ハウス１０５は、オーダＳＣ６５０を妥当性検査して処理し、ライセンス・ウォータマーク５２７に対して必要で、かつ購入したコンテンツ１１３にアクセスするために必要なあらゆるものをエンドユーザ装置１０９に提供する。クリアリング・ハウス１０５の機能の１つは、オファーＳＣ６４１からのウォータマーク命令とコンテンツＳＣ６３０からのコンテンツ１１３を暗号化解除するのに必要な対称キー６２３を暗号化解除することである。暗号化対称キー６２３のレコードは、実際には、実際の暗号化対称キー６２３以上のものを含んでいる。暗号化を実行する前に、コンテンツ・プロバイダ１０１は任意選択でその名前を実際の対称キー６２３に付加することができる。対称キー６２

３とともにコンテンツ・プロバイダ１０１の名前が暗号化されているので、合法的ＳＣからそれ自身のメタデータＳＣ６２０とコンテンツＳＣ６３０を構築した著作権侵害コンテンツ・プロバイダ１０１から保護される。クリアリング・ハウス１０５は、対称キー６２３とともに暗号化されたコンテンツ・プロバイダ１０１の名前がＳＣ証書内のコンテンツ・プロバイダ１０１の名前と一致することを検証する。

【０１１５】クリアリング・ハウス１０５によってウォータマーク命令に対して何らかの変更を行う必要がある場合、クリアリング・ハウス１０５は対称キー６２３を暗号化解除し、次にウォータマーク命令を変更し、新しい対称キー６２３を使用してそれをもう一度暗号化する。その後、対称キー６２３は、エンドユーザ装置１０９の公開キー６６１を使用して再暗号化される。また、クリアリング・ハウス１０５は、ＳＣ内の他の対称キー６２３も暗号化解除し、エンドユーザ装置１０９の公開キー６６１でそれをもう一度暗号化する。クリアリング・ハウス１０５は、新たに暗号化した対称キー６２３と更新したウォータマーク命令を含むライセンスＳＣ６６０を構築し、オーダＳＣ６５０に応答してそれをエンドユーザ装置１０９に送る。オーダＳＣ６５０の処理が正常に完了しない場合、クリアリング・ハウス１０５は認可プロセスの失敗を報告するＨＴＭＬページまたは同等のものをエンドユーザ装置１０９に返す。

【０１１６】ライセンスＳＣ６６０は、コンテンツ１１３の項目にアクセスするために必要なあらゆるものをエンドユーザ装置１０９に提供する。エンドユーザ装置１０９はコンテンツ・ホスト・サイト１１１から適切なコンテンツＳＣ６３０を要求する。コンテンツＳＣ６３０は、コンテンツ・プロバイダ１０１によって構築され、暗号化コンテンツ１１３とメタデータ・パーツを含む。エンドユーザ・プレーヤ・アプリケーション１９５は、ライセンスＳＣ６６０からの対称キー６２３を使用して、コンテンツ１１３、メタデータ、ウォータマーク命令を暗号化解除する。次に、ウォータマーク命令はコンテンツ１１３内に添付され、コンテンツ１１３はスクランブルされてエンドユーザ装置１０９に記憶される。

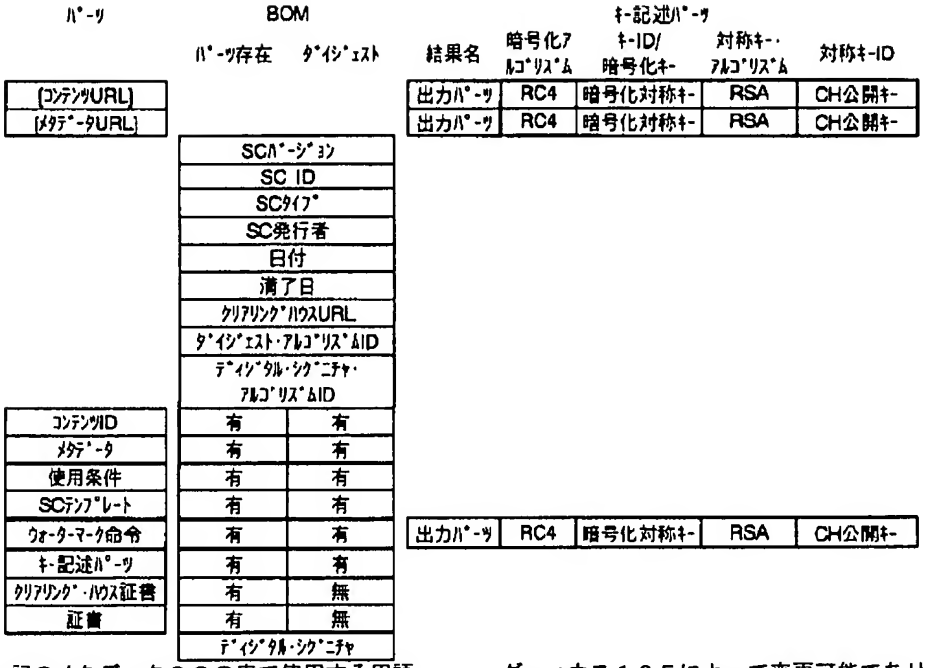
【０１１７】Ｄ．メタデータ・セキュア・コンテナ６２０のフォーマット

以下の表はメタデータＳＣ６２０に含まれるパーツを示している。パーツ列の各ボックスは、ＢＯＭとともにＳＣに含まれる個別のオブジェクトである（［］という文字で囲まれたパーツ名は除く）。ＢＯＭはＳＣに含まれる各パーツのレコードを含む。パーツ存在列はそのパーツ自体が実際にＳＣに含まれているかどうかを示し、ダイジェスト列はそのパーツについてメッセージ・ダイジェストが計算されるかどうかを示す。元のＢＯＭ全体は伝播されるが、（関連テンプレートによって決定されるように）あるＳＣが他のＳＣに含まれるとパーツによっては伝播されない場合がある。これは、元のＳＣ内のディジタル・シグニチャを検証するためにクリアリング・ハウス１０５がＢＯＭ全体を必要とするためである。

【０１１８】以下の表のキー記述パーツ列は、ＳＣのキー記述パーツに含まれるレコードを定義するものである。キー記述パーツ内のレコードは、そのＳＣ内のパーツまたは他のＳＣ内のパーツを暗号化するために使用した暗号化キーおよびアルゴリズムに関する情報を定義する。各レコードは、暗号化パーツ名と、必要であれば、その暗号化パーツを含む他のＳＣを指し示すＵＲＬとを含む。結果名列は、それが暗号化解除された後でそのパーツに割り当てられる名前を定義する。暗号化アルゴリズム列は、そのパーツを暗号化するために使用した暗号化アルゴリズムを定義する。キーＩＤ／暗号化キー列は、そのパーツを暗号化するために使用した暗号化キーの識別名またはそのパーツを暗号化するために使用した暗号化対称キー６２３のビット・ストリングのベース６４コード化のいずれかを定義する。対称キー・アルゴリズム列は、前の列が暗号化対称キー６２３であるときに対称キー６２３を暗号化するために使用した暗号化アルゴリズムを定義する任意選択のパラメータである。対称キーＩＤ列は、キーＩＤ／暗号化キー列が暗号化対称キー６２３であるときに対称キー６２３を暗号化するために使用した暗号化キーの識別名である。

【０１１９】

【表３】



【０１２０】上記のメタデータＳＣの表で使用する用語について以下に説明する。

・　［コンテンツＵＲＬ］　－　キー記述パーツのレコード内のパラメータ。これは、コンテンツＳＣ６３０内にあってこのメタデータＳＣ６２０に関連する暗号化コンテンツ１１３を指し示すＵＲＬである。メタデータＳＣ６２０自体は暗号化コンテンツ１１３を含まない。

・　［メタデータＵＲＬ］　－　キー記述パーツのレコード内のパラメータ。これは、コンテンツＳＣ６３０内にあってこのメタデータＳＣ６２０に関連する暗号化メタデータを指し示すＵＲＬである。メタデータＳＣ６２０自体は暗号化メタデータを含まない。

・　コンテンツＩＤ　－　コンテンツ１１３の項目に割り当てられた固有のＩＤを定義するパーツ。メタデータＳＣ６２０がコンテンツ１１３の複数の項目を参照する場合、このパーツ内に複数のコンテンツＩＤが含まれる。

・　メタデータ　－　歌曲の場合はアーチスト名およびＣＤカバー・アートなどのコンテンツ１１３の項目に関する情報を含むパーツ。複数のメタデータ・パーツが存在する可能性があり、そのうちの一部が暗号化可能である。メタデータ・パーツの内部構造はそこに含まれるメタデータのタイプに依存する。

・　使用条件　－　コンテンツ１１３の使用のためにエンドユーザに課せられる使用オプション、規則、制限を記述する情報を含むパーツ。

・　ＳＣテンプレート　－　オファー、オーダ、ライセンスの各ＳＣ６６０を構築するための必須情報および任意選択情報を記述するテンプレートを定義するパーツ。

・　ウォータマーク命令　－　コンテンツ１１３内でウォータマークを実施するための暗号化命令およびパラメータを含むパーツ。ウォータマーク命令は、クリアリング・ハウス１０５によって変更可能であり、ライセンスＳＣ６６０内でエンドユーザ装置１０９に返すことができる。ウォータマーク命令を暗号化するために使用した暗号化アルゴリズム、ウォータマーク命令を暗号化解除するときに使用する出力パーツ名、ウォータマーク命令を暗号化するために使用した暗号化対称キー６２３のビット・ストリングのベース６４コード化、対称キー６２３を暗号化するために使用した暗号化アルゴリズム、対称キー６２３を暗号化解除するために必要な公開キーの識別名を定義するレコードがキー記述パーツ内に存在する。

・　クリアリング・ハウス証書　－　クリアリング・ハウス１０５のサイン付き公開キー６２１を含む、証明機関からまたはクリアリング・ハウス１０５からの証書。複数の証書が存在する可能性があり、その場合、階層レベル構造が使用され、二番目に高いレベルの証書をオープンするための公開キーを含む最高レベルの証書が届けられ、それはクリアリング・ハウス１０５の公開キー６２１を含む。

・　証書　－　ＳＣを作成したエンティティのサイン付き公開キー６２１を含む、証明機関からまたはクリアリング・ハウス１０５からの証書。複数の証書が存在する可能性があり、その場合、階層レベル構造を使用し、ＳＣ作成者の公開キー６２１を含む最低レベルの証書に達するまで、最高レベルの証書は次のレベルの証書などをオープンするための公開キーを含む。

・　ＳＣバージョン　－　ＳＣパッカ・ツールによってＳＣに割り当てられたバージョン番号。

・　ＳＣ　ＩＤ　－　ＳＣを作成したエンティティによってそのＳＣに割り当てられた固有のＩＤ。

・　ＳＣタイプ　－　ＳＣのタイプ（たとえば、メタデータ、オファー、オーダなど）を示す。

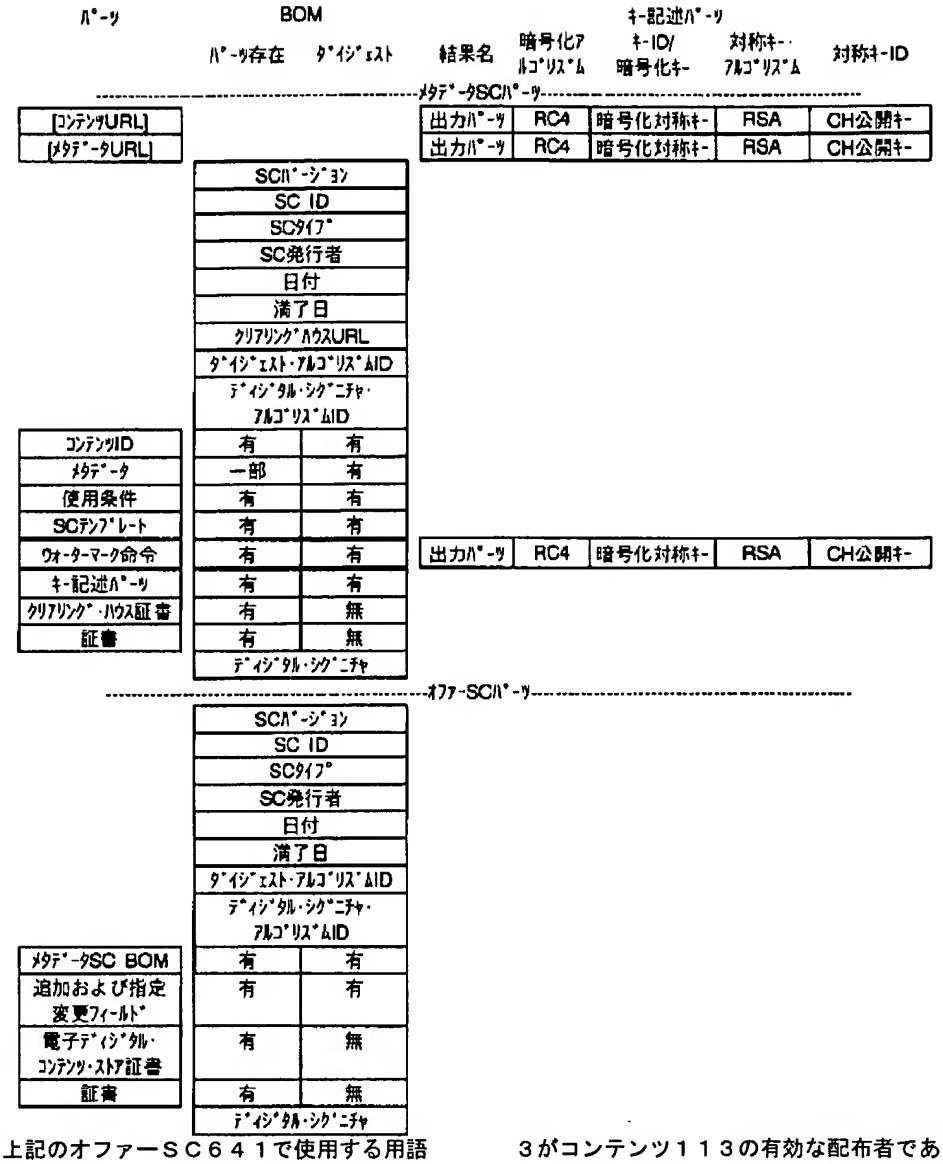
・　ＳＣ発行者　－　ＳＣを作成したエンティティを示す。
・　作成日　－　ＳＣが作成された日付。
・　満了日　－　ＳＣが満期になり、もはや有効ではなくなる日付。
・　クリアリング・ハウスＵＲＬ　－　コンテンツ１１３にアクセスするための適正な認可を得るためにエンドユーザ・プレーヤ・アプリケーション１９５が対話しなければならないクリアリング・ハウス１０５のアドレス。
・　ダイジェスト・アルゴリズムＩＤ　－　パーツのダイジェストを計算するために使用するアルゴリズムの識別子。
・　ディジタル・シグニチャ・アルゴリズムＩＤ　－　連結パーツ・ダイジェストのダイジェストを暗号化するために使用するアルゴリズムの識別子。この暗号化値はディジタル・シグニチャである。
・　ディジタル・シグニチャ　－　ＳＣを作成したエンティティの公開キーで暗号化した連結パーツ・ダイジェストのダイジェスト。
・　出力パーツ　－　暗号化パーツを暗号化解除するときに出力パーツに割り当てる名前。
・　ＲＳＡおよびＲＣ４　－　対称キー６２３とデータ・パーツを暗号化するために使用するデフォルト暗号化アルゴリズム。
・　暗号化対称キー　－　暗号化解除したときにＳＣパーツを暗号化解除するために使用する暗号化キー・ビット・ストリングのベース６４コード化。
・　ＣＨ公開キー　－　クリアリング・ハウス１０５の公開キー６２１を使用してそのデータを暗号化したことを示す識別子。

【０１２１】Ｅ．オファー・セキュア・コンテナ６４１のフォーマット

以下の表はオファーＳＣ６４１に含まれるパーツを示している。メタデータ・パーツの一部を除くパーツと、メタデータＳＣ６２０からのＢＯＭもオファーＳＣ６４１に含まれる。

【０１２２】

【表４】



【０１２３】上記のオファーＳＣ６４１で使用する用語のうち、他のＳＣに関して前述していない用語について以下に説明する。

・　メタデータＳＣＢＯＭ　－　元のメタデータＳＣ６２０からのＢＯＭ。オファーＳＣ６４１のＢＯＭ内のレコードはメタデータＳＣ６２０のＢＯＭのダイジェストを含む。

・　追加および指定変更フィールド　－　電子ディジタル・コンテンツ・ストア１０３によって指定変更された使用条件情報。受け取ったＳＣテンプレートによりクリアリング・ハウス１０５がこの情報を妥当性検査し、電子ディジタル・コンテンツ・ストア１０３が指定変更するものはいずれもその認可の範囲内であることを確認する。

・　電子ディジタル・コンテンツ・ストア証書　－　クリアリング・ハウス１０５によって電子ディジタル・コンテンツ・ストア１０３に提供され、その秘密キーを使用してクリアリング・ハウス１０５がサインした証書。この証書は、電子ディジタル・コンテンツ・ストア１０３がコンテンツ１１３の有効な配布者であることを検証するためにエンドユーザ・プレーヤ・アプリケーション１９５が使用する。エンドユーザ・プレーヤ・アプリケーション１９５とクリアリング・ハウス１０５は、クリアリング・ハウス１０５の公開キー６２１で証書のシグニチャを暗号化解除することにより、電子ディジタル・コンテンツ・ストア１０３が認可配布者であることを検証することができる。エンドユーザ・プレーヤ・アプリケーション１９５は、それがインストール時にその初期設定の一部として受け取るクリアリング・ハウス１０５の公開キー６２１のローカル・コピーを保持する。

【０１２４】Ｆ．トランザクション・セキュア・コンテナ６４０のフォーマット

以下の表はトランザクションＳＣ６４０に含まれるパーツならびにそのＢＯＭおよびキー記述パーツを示している。

【０１２５】

【表５】

パーツ	BOM			キー記述パーツ			
	パーツ存在	ダイジェスト	結果名	暗号化アルゴリズム	キーID/暗号化キー	対称キー・アルゴリズム	対称キーID
		SCバージョン					
		SC ID					
		SCタイプ					
		SC発行者					
		日付					
		満了日					
		ダイジェスト・アルゴリズムID					
		デジタル・シグニチャ・アルゴリズムID					
トランザクションID	有	有	出力パーツ	RSA	CH公開キー		
エンドユーザID	有	有	出力パーツ	RSA	CH公開キー		
エンドユーザの公開キー	有	有					
オファーSC	有	有					
コンテンツ使用の選択	有	有					
表示用HTML	有	有					
キー記述パーツ	有	有					
電子ディジタル・コンテンツ・ストア証書	有	無					
		デジタル・シグニチャ					

【０１２６】上記のトランザクションＳＣ６４０で使用する用語のうち、他のＳＣに関して前述していない用語について以下に説明する。

・　トランザクションＩＤ５３５　－　トランザクションを明確に識別するために電子ディジタル・コンテンツ・ストア１０３によって割り当てられるＩＤ。

・　エンドユーザＩＤ　－　エンドユーザが購入選択を行い、クレジット・カード情報を提供したときに電子ディジタル・コンテンツ・ストア１０３が取得するエンドユーザの識別名。

・　エンドユーザの公開キー　－　対称キー６２３を再暗号化するためにクリアリング・ハウス１０５が使用するエンドユーザの公開キー６６１。エンドユーザの公開キー６６１は購入トランザクション中に電子ディジタル・コンテンツ・ストア１０３に伝送される。

・　オファーＳＣ　－　購入されたコンテンツ１１３の項目に関するオファーＳＣ６４１。

・　コンテンツ使用の選択　－　エンドユーザが購入するコンテンツ１１３の各項目ごとの使用条件のアレイ。各オファーＳＣ６４１ごとに１つの項目が存在する。

・　表示用ＨＴＭＬ　－　トランザクションＳＣ６４０を受け取った後またはエンドユーザ装置１０９とクリアリング・ハウス１０５との対話中にエンドユーザ・プレーヤ・アプリケーション１９５がインターネット・ブラウザのウィンドウ内に表示する１つまたは複数のＨＴＭＬページ。

【０１２７】エンドユーザ装置１０９がトランザクションＳＣ６４０を受け取った場合、ＳＣの完全性と信憑性を検証するために以下のステップを実行することができる。

１．クリアリング・ハウス１０５の公開キー６２１を使用して電子ディジタル・コンテンツ・ストア１０３の証書の完全性を検証する。クリアリング・ハウス１０５の公開キー６２１は、そのインストール・プロセス中にエンドユーザ・プレーヤ・アプリケーション１９５の初期設定の一部として受け取られた後、エンドユーザ装置１０９に記憶されている。

２．電子ディジタル・コンテンツ・ストア１０３の証書からの公開キーを使用してＳＣのディジタル・シグニチャ６４３を検証する。

３．ＳＣパーツのハッシュを検証する。

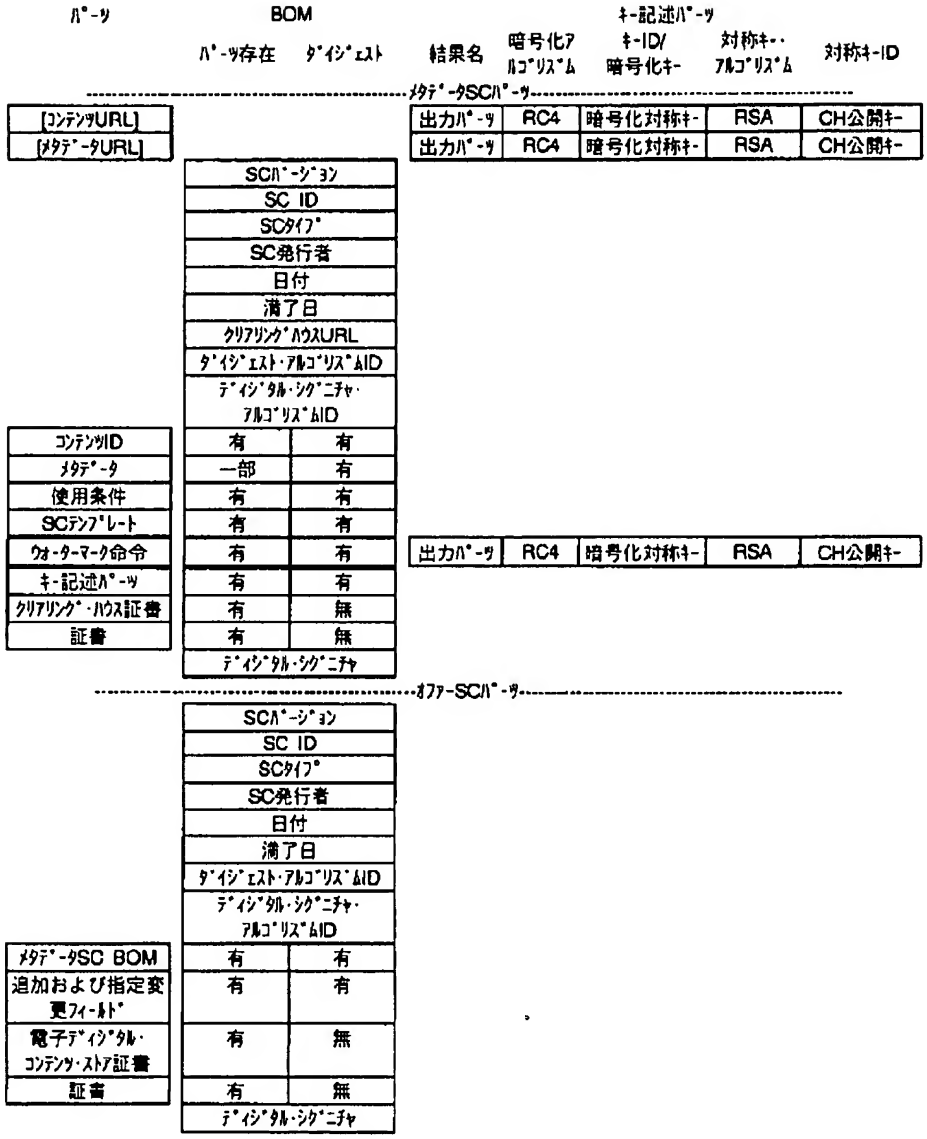
４．トランザクションＳＣ６４０に含まれる各オファーＳＣ６４１の完全性と信憑性を検証する。

【０１２８】Ｇ．オーダ・セキュア・コンテナ６５０のフォーマット

以下の表はオーダＳＣ６５０に含まれるパーツならびにそのＢＯＭおよびキー記述パーツを示している。これらのパーツは、暗号化解除および検証のためにクリアリング・ハウス１０５に情報を提供するか、またはクリアリング・ハウス１０５によって妥当性検査される。オファーＳＣ６４１からのパーツおよびＢＯＭもオーダＳＣ６５０に含まれる。メタデータＳＣのＢＯＭのパーツ存在列内の一部という文字列は、これらのパーツの一部がオーダＳＣ６５０に含まれないことを示している。クリアリング・ハウス１０５がメタデータＳＣ６２０とそのパーツの完全性を妥当性検査できるように何らかの変更を行わずに、メタデータＳＣ６２０からのＢＯＭも含まれる。

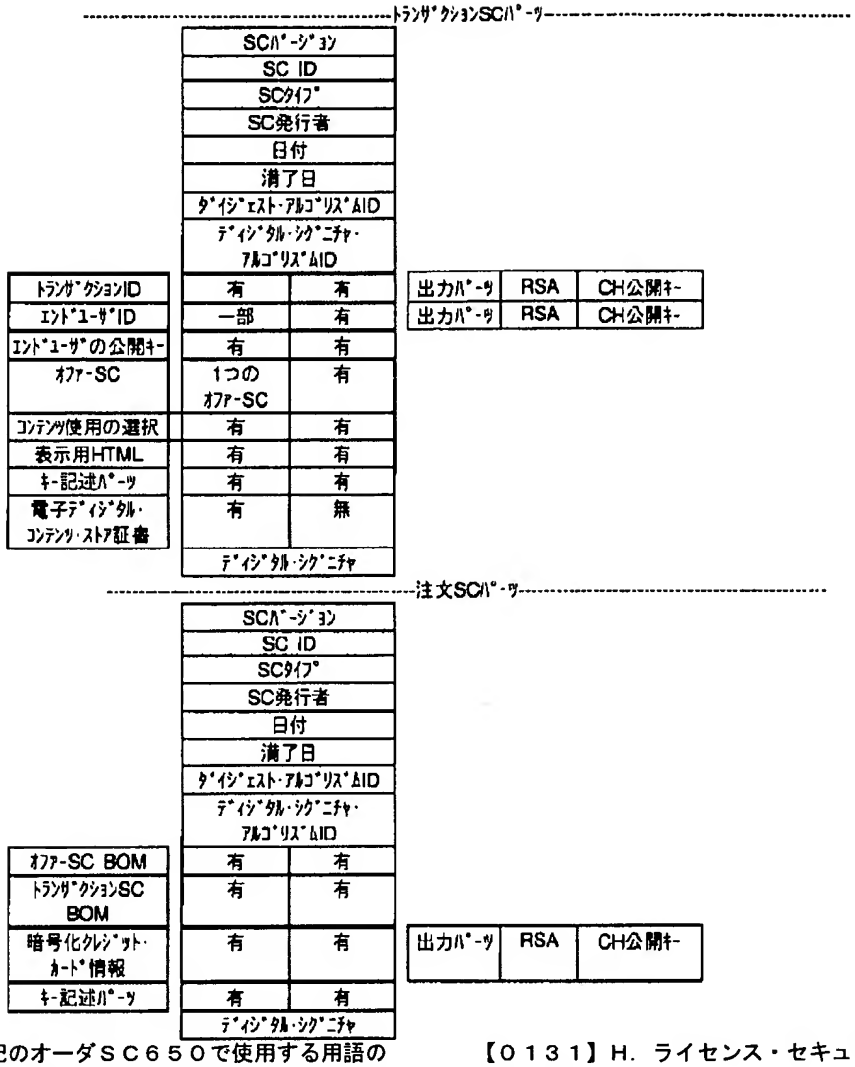
【０１２９】

【表６】


パーツ
BOM
キー記述パーツ
パーツ存在
ダイジェスト
結果名
暗号化アルゴリズム
キーID/暗号化キー
対称キー・アルゴリズム
対称キーID
メタデータSCパーツ
[コンテンツURL]
[メタデータURL]
出力パーツ
RC4
暗号化対称キー
RSA
CH公開キー
出力パーツ
RC4
暗号化対称キー
RSA
CH公開キー
SCバージョン
SC ID
SCタイプ
SC発行者
日付
満了日
クリアリングハウスURL
ダイジェスト・アルゴリズムID
ディジタル・シグニチャ・アルゴリズムID
コンテンツID
有
有
メタデータ
一部
有
使用条件
有
有
SCテンプレート
有
有
ウォーターマーク命令
有
有
出力パーツ
RC4
暗号化対称キー
RSA
CH公開キー
キー記述パーツ
有
有
クリアリング・ハウス証書
有
無
証書
有
無
ディジタル・シグニチャ
オファーSCパーツ
SCバージョン
SC ID
SCタイプ
SC発行者
日付
満了日
ダイジェスト・アルゴリズムID
ディジタル・シグニチャ・アルゴリズムID
メタデータSC BOM
有
有
追加および指定変更フィールド
有
有
電子ディジタル・コンテンツ・ストア証書
有
無
証書
有
無
ディジタル・シグニチャ

【表７】

（表６の続き）



【０１３０】上記のオーダＳＣ６５０で使用する用語のうち、他のＳＣに関して前述していない用語について以下に説明する。

・　トランザクションＳＣＢＯＭ　－　元のトランザクションＳＣ６４０内のＢＯＭ。オーダＳＣ６５０のＢＯＭ内のレコードはトランザクションＳＣ６４０のＢＯＭのダイジェストを含む。

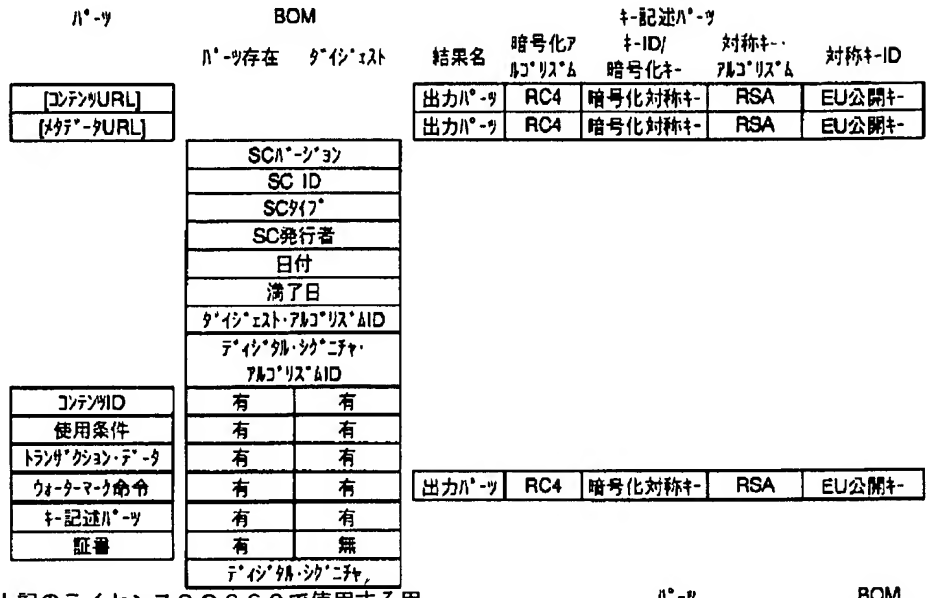
・　暗号化クレジット・カード情報　－　その購入をクレジット・カードまたはデビット・カードに請求するために使用する、エンドユーザからの任意選択の暗号化情報。この情報は、オファーＳＣ６４１を作成した電子ディジタル・コンテンツ・ストア１０３が顧客請求を処理しないときに必要になり、その場合、クリアリング・ハウス１０５がその請求を処理することができる。

【０１３１】Ｈ．ライセンス・セキュア・コンテナ６６０のフォーマット

以下の表はライセンスＳＣ６６０に含まれるパーツならびにそのＢＯＭを示している。キー記述パーツに示すように、ウォータマーク命令、コンテンツ１１３、コンテンツ１１３のメタデータを暗号化解除するために必要な対称キー６２３は、エンドユーザの公開キー６６１を使用してクリアリング・ハウス１０５によって再暗号化されている。エンドユーザ装置１０９がライセンスＳＣ６６０を受け取ると、それは対称キー６２３を暗号化解除し、それらを使用してライセンスＳＣ６６０およびコンテンツＳＣ６３０からの暗号化パーツにアクセスする。

【０１３２】

【表８】



【０１３３】上記のライセンスＳＣ６６０で使用する用語のうち、他のＳＣに関して前述していない用語について以下に説明する。

・　ＥＵ公開キー　－　エンドユーザの公開キー６６１を使用してそのデータを暗号化したことを示す識別子。

・　オーダＳＣ６５０のＩＤ　－　オーダＳＣ６５０のＢＯＭから取得したＳＣのＩＤ。

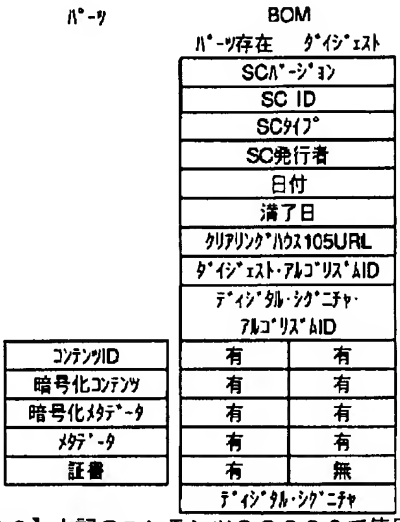
・　証書撤回リスト　－　クリアリング・ハウス１０５によって前に発行され、サインされたが、もはや有効とは見なされない証書ＩＤの任意選択のリスト。撤回リストに含まれる証書によって検証可能なシグニチャを有するＳＣは無効ＳＣである。エンドユーザ・プレーヤ・アプリケーション１９５はクリアリング・ハウス１０５の証書撤回リストのコピーをエンドユーザ装置１０９に記憶する。撤回リストを受け取ると、エンドユーザ・プレーヤ・アプリケーション１９５は、新しいリストがより最新のものである場合、そのローカル・コピーを置き換える。撤回リストは、どのリストが最も最新ものであるかを判定するために、バージョン番号またはタイム・スタンプ（あるいはその両方）を含む。

【０１３４】Ｉ．コンテンツ・セキュア・コンテナのフォーマット

以下の表はコンテンツＳＣ６３０に含まれるパーツならびにそのＢＯＭを示している。

【０１３５】

【表９】



【０１３６】上記のコンテンツＳＣ６３０で使用する用語のうち、他のＳＣに関して前述していない用語について以下に説明する。

・　暗号化コンテンツ　－　対称キー６２３を使用してコンテンツ・プロバイダ１０１によって暗号化されたコンテンツ１１３。

・　暗号化メタデータ　－　コンテンツ１１３に関連するメタデータのうち、対称キー６２３を使用してコンテンツ・プロバイダ１０１によって暗号化されたメタデータ。

【０１３７】暗号化パーツを暗号化解除するために必要なキーはクリアリング・ハウス１０５で構築されたライセンスＳＣ６６０内にあるので、コンテンツＳＣ６３０にはキー記述パーツは一切含まれない。

【０１３８】ＶＩ．セキュア・コンテナのパックおよびアンパック

Ａ．概要

ＳＣのパッカは、指定のパーツのすべてを使ってＳＣを作成するために複数または単一ステップ・プロセスで呼び出すことができ、ＡＰＩ（アプリケーション・プログ

ラミング・インタフェース）を備えた３２ビットのWindowsプログラムである。ＳＣのパッカ１５１、１５２、１５３は、コンテンツ・プロバイダ１０１、クリアリング・ハウス１０５、電子ディジタル・コンテンツ・ストア１０３、ＳＣのパックを必要とするその他のサイトでWindowsプログラムをサポートする様々なハードウェア・プラットフォームである。ＢＯＭと、必要であればキー記述パーツが作成され、ＳＣに含まれる。１組のパッカＡＰＩにより、呼出し側は、ＢＯＭおよびキー記述パーツ内のレコードを生成し、ＳＣにパーツを含めるのに必要な情報を指定することができる。パーツおよび対称キー６２３の暗号化ならびにダイジェストおよびディジタル・シグニチャの計算もパッカによって実行される。パッカがサポートする暗号化およびダイジェスト・アルゴリズムはパッカ・コードに含まれるかまたは外部インタフェースを介して呼び出される。

【０１３９】ＳＣを構築するためのパッカへのインタフェースは１つのＡＰＩによって行われ、そのＡＰＩは以下のパラメータを入力として受け入れる。

・　連結構造のバッファを指し示すポインタ。バッファ内の各構造は、パッカへのコマンドであり、そのコマンドを実行するのに必要な情報を伴う。パッカ・コマンドとしては、関連ＢＯＭレコードを備えたＳＣにパーツを追加すること、ＢＯＭにレコードを追加すること、キー記述パーツにレコードを追加することを含む。

・　上記のバッファに含まれる連結構造の数を示す値。

・　ＢＯＭパーツの名前および位置。

・　各ビットが定義済みフラグまたは今後の使用のための予約済みフラグである値。現在、以下のフラグが定義されている。

－　バッファ内のすべての構造が処理された後でＳＣのすべてのパーツをまとめてバンドルして単一ファイルにしなければならないかどうかに関する表示。全パーツを単一オブジェクトにバンドルすることは、ＳＣを構築するときに実行する最後のステップである。

－　ディジタル・シグニチャがＢＯＭパーツから省略されているかどうかに関する表示。このフラグが設定されていない場合、ＳＣが単一オブジェクトにバンドルされる直前にディジタル・シグニチャが計算される。

【０１４０】代替実施形態では、ＳＣを構築するためのパッカへのインタフェースは複数ＡＰＩによって行われ、そのＡＰＩは以下のパラメータを入力として受け入れる。

・　まず、ＳＣのＢＯＭパーツ内でＩＰレコードとして示されるＳＣの設定を初期設定するために使用する情報からなる構造を指し示すポインタとして、ＢＯＭパーツに使用するための名前と、追加されるパーツを探すためのデフォルト位置と、フラグ値とを渡すことにより、素材一覧表（ＢＯＭ）パーツを作成するためにＡＰＩが呼び出される。このＡＰＩは、後続パッカＡＰＩで使用するＳＣハンドルを返す。

・　このパッカは、ＳＣにパーツが追加されるときに必ず使用するＡＰＩを有する。このＡＰＩは、前のパッカＡＰＩから事前に返されたＳＣハンドルと、追加されるパーツに関する情報からなる構造を指し示すポインタと、フラグ値とを受け入れる。追加されるパーツに関する情報としては、そのパーツの名前および位置、ＢＯＭ内でそのパーツに使用するための名前、追加されるパーツのタイプ、そのパーツ用のハッシュ値、フラグなどを含む。

・　すべてのパーツがＳＣに追加された後で、ＢＯＭパーツを含むすべてのパーツを、通常はファイルである単一ＳＣオブジェクトにパックするためにパッカＡＰＩが呼び出される。このＡＰＩは、前のパッカＡＰＩから事前に返されたＳＣハンドルと、パックしたＳＣに使用するための名前と、そのＳＣにサインするための情報を備えた構造を指し示すポインタと、フラグ値とを受け入れる。

【０１４１】パッカまたはパッカを呼び出すエンティティは、ＳＣテンプレートを使用してＳＣを構築することができる。ＳＣテンプレートは、構築中のＳＣで必要なパーツおよびレコードを定義する情報を有する。また、テンプレートは、暗号化対称キー６２３および暗号化パーツに使用するための暗号化方法およびキー参照も定義することができる。

【０１４２】パッカは、ＳＣをアンパックするために使用するＡＰＩを有する。ＳＣのアンパックは、ＳＣを取得し、それを個々のパーツに分離するプロセスである。その後、そのパッカを呼び出して、ＳＣからアンパックされた暗号化パーツのいずれかを暗号化解除することができる。

【０１４３】Ｂ．素材一覧表（ＢＯＭ）パーツ

ＢＯＭパーツは、ＳＣを構築するときにパッカによって作成される。ＢＯＭは、ＳＣとそのＳＣに含まれるパーツに関する情報のレコードを含むテキスト・ファイルである。ＢＯＭ内の各レコードは単一行上にあり、新しいレコードの開始は新しい行が示す。通常、ＢＯＭは、各パーツのダイジェストと、そのＳＣの信憑性および完全性を妥当性検査するために使用可能なディジタル・シグニチャとを含む。

【０１４４】ＢＯＭ内のレコード・タイプは以下の通りである。

ＩＰ　ＩＰレコードは、そのＳＣに関係する１組の名前＝値の対を含む。ＳＣの特定のプロパティのために以下の名前が予約されている。

V major.minor.fix

Ｖプロパティは ＳＣのバージョンを指定する。これは、ＳＣが作成されたときのＳＣ仕様のバージョン番号である。後続の文字列は、major.minor.fixという形式でなければならず、major、minor、fixはそれぞれメジャー

・リリース番号、マイナ・リリース番号、修正レベルである。
ID value
ＩＤプロパティは、このＳＣを作成するエンティティがこの特定のＳＣに割り当てる固有の値である。この値のフォーマットは本書の今後のバージョンで定義される。
T value
ＴプロパティはＳＣのタイプを指定し、以下のいずれか１つでなければならない。
ＯＲＤ　－　オーダＳＣ６５０
ＯＦＦ　－　オファーＳＣ６４１
ＬＩＣ　－　ライセンスＳＣ
ＴＲＡ　－　トランザクションＳＣ６４０
ＭＥＴ　－　メタデータＳＣ６２０
ＣＯＮ　－　コンテンツＳＣ６３０
A value
ＡプロパティはＳＣの作成者または発行者を識別する。作成者／発行者のアイデンティティは、明白なものであるかまたはクリアリング・ハウス１０５に登録しなければならない。
D value
Ｄプロパティは、ＳＣが作成された日付と、任意選択で時刻を識別する。この値は、年／月／日@時：分：秒.小数秒（時間帯）を表すyyyy/mm/dd[@hh:mm[:ss[.fsec]][(TZ)]]という形式でなければならない。この値の任意選択部分は [] という文字で囲まれている。
E value
Ｅプロパティは、ＳＣが満期になる日付と、任意選択で時刻を識別する。この値は、前に定義したＤプロパティで使用するのと同じ形式でなければならない。満了日／時刻は、可能であれば必ず、クリアリング・ハウス１０５での日付／時刻と比較しなければならない。
CCURL value
ＣＣＵＲＬプロパティはクリアリング・ハウス１０５のＵＲＬを識別する。この値は、有効な外部ＵＲＬの形式でなければならない。
H value
Ｈプロパティは、ＳＣに含まれるパーツ用のメッセージ・ダイジェストを計算するために使用したアルゴリズムを識別する。ダイジェスト・アルゴリズムの一例はＭＤ５である。
Ｄ　Ｄレコードは、パーツのタイプ、パーツの名前、パーツの（任意選択の）ダイジェスト、そのパーツがＳＣに含まれないという（任意選択の）表示を識別する情報を含むデータまたはパーツ項目レコードである。タイプ識別子の直後の－符号は、そのパーツがＳＣに含まれないことを示すために使用する。データまたはパーツ・レコードの予約済みタイプは以下の通りである。
K part_name [digest]
キー記述パーツを指定する。
W part_name [digest]
ウォータマーク命令パーツを指定する。
C part_name [digest]
ディジタル・シグニチャを妥当性検査するために使用する証書を指定する。
T part_name [digest]
使用条件パーツを指定する。
YF part_name [digest]
オファーＳＣ６４１用のテンプレート・パーツを指定する。
YO part_name [digest]
オーダＳＣ６５０用のテンプレート・パーツを指定する。YL part_name [digest]
ライセンスＳＣ６６０用のテンプレート・パーツを指定する。
ID part_name [digest]
参照中のコンテンツ１１３の項目のコンテンツ１１３のＩＤを指定する。
CH part_name [digest]
クリアリング・ハウス１０５の証書パーツを指定する。
SP part_name [digest]
電子ディジタル・コンテンツ・ストア１０３の証書パーツを指定する。
B part_name [digest]
このＳＣに含まれるそのパーツまたはそのパーツのサブセットを有する他のＳＣのＢＯＭパーツを指定する。
BP part_name sc_part_name [digest]
単一パーツとしてこのＳＣに含まれる他のＳＣのＢＯＭパーツを指定する。sc_part_nameというパラメータは、このＳＣに含まれ、このＢＯＭパートが定義するＳＣパーツの名前である。これと同一のＢＯＭも、sc_part_nameパラメータによって定義されるＳＣに含まれる。
D part_name [digest]
データ（またはメタデータ）パーツを指定する。
Ｓ　Ｓレコードは、ＳＣのディジタル・シグニチャを定義するために使用するシグニチャ・レコードである。ディジタル・シグニチャは以下のように指定される。
S key_identifier signature_string signature_algorithm
Ｓレコードは、シグニチャの暗号化キーを示すためのkey_identifierと、ディジタル・シグニチャ・ビットストリングのベース６４コード化であるsignature_stringと、ダイジェストを暗号化してディジタル・シグニチャを作成するために使用したsignature_algorithmとを含む。
【０１４５】Ｃ．キー記述パーツ
キー記述パーツは、ＳＣの暗号化パーツの暗号化解除のために必要な暗号化キーに関する情報を提供するためにパッカによって作成される。暗号化パーツは、構築中のＳＣに含まれる場合もあれば、構築中のＳＣが参照する

他のＳＣに含まれる場合もある。キー記述パーツは、暗号化キーと、その暗号化キーが使用されたパーツに関する情報のレコードを含むテキスト・ファイルである。キー記述パーツ内の各レコードは単一行上にあり、新しいレコードの開始は新しい行が示す。

【０１４６】以下のレコード・タイプは、キー記述パーツ内で使用され、以下のように定義される。

K　encrypted_part_name ; result_part_name ; part_encryption_algorithm_identifier ; public_key_identifier ; key_encryption_algorithm ; encrypted_symmetric_key

Kレコードは、このＳＣに含まれる可能性があるかまたはこのレコードが参照する他のＳＣに含まれる可能性のある暗号化パーツを指定する。encrypted_part_nameは、このＳＣ内のパーツの名前かまたは他のＳＣ内の暗号化パーツの名前を指し示すＵＲＬのいずれかである。result_part_nameは、暗号化解除したパーツに与えられる名前である。part_encryption_algorithm_identifierは、そのパーツを暗号化するために使用した暗号化アルゴリズムを示す。public_key_identifierは、対称キー６２３を暗号化するために使用したキーの識別子である。key_encryption_algorithmは、対称キー６２３を暗号化するために使用した暗号化アルゴリズムを示す。encrypted_symmetric_keyは、そのパーツを暗号化するために使用した暗号化対称キー６２３のビット・ストリングのベース６４コード化である。

【０１４７】VII. クリアリング・ハウス１０５

Ａ. 概要

クリアリング・ハウス１０５は、セキュア・ディジタル・コンテンツ電子配布システム１００の権利管理機能を担当する。クリアリング・ハウス１０５の機能としては、電子ディジタル・コンテンツ・ストア１０３を使用可能にすること、コンテンツ１１３に対する権利を検証すること、購入トランザクションおよび関連情報の完全性および信憑性を妥当性検査すること、コンテンツ暗号化キーまたは対称キー６２３をエンドユーザ装置１０９に配布すること、これらのキーの配布を追跡すること、電子ディジタル・コンテンツ・ストア１０３およびコンテンツ・プロバイダ１０１にトランザクション要約を報告することを含む。コンテンツ暗号化キーは、通常は認可電子ディジタル・コンテンツ・ストア１０３からの購入トランザクションによってエンドユーザ装置がそれに関する権利を取得したコンテンツ１１３をロック解除するためにエンドユーザ装置１０９が使用する。コンテンツ暗号化キーがエンドユーザ装置１０９に送られる前に、クリアリング・ハウス１０５は、検証プロセスを経て、コンテンツ１１３を販売するエンティティの信憑性と、エンドユーザ装置１０９がそのコンテンツ１１３に対して持っている権利を妥当性検査する。これはＳＣ分析ツール１８５と呼ばれる。一部の構成では、クリアリング・ハウス１０５は、クレジット・カード認証および請求という電子ディジタル・コンテンツ・ストア１０３の機能を実行するシステムをクリアリング・ハウス１０５に併置することにより、購入したコンテンツ１１３の金融決済も処理することができる。クリアリング・ハウス１０５では、ICVerifyおよびTaxwareなどのＯＥＭパッケージを使用して、クレジット・カードの処理および地域の売上税を処理する。

【０１４８】電子ディジタル・コンテンツ・ストアの実施形態

セキュア・ディジタル・コンテンツ電子配布システム１００においてコンテンツ１１３の販売者として関与することを希望する電子ディジタル・コンテンツ・ストア１０３は、セキュア・ディジタル・コンテンツ電子配布システム１００にコンテンツ１１３を提供するディジタル・コンテンツ・プロバイダ１０１の１つまたは複数に対して要求を行う。２人の当事者が合意に達する限り、要求を行うための決定的なプロセスはまったくない。電子ディジタル・コンテンツ・ストア１０３がそのコンテンツ１１３を販売できるようにすることをたとえばソニー、タイムワーナーなどの音楽レーベルなどのディジタル・コンテンツ・レーベルが決定した後、クリアリング・ハウス１０５は通常はＥメールを介して、電子ディジタル・コンテンツ・ストア１０３をセキュア・ディジタル・コンテンツ電子配布システム１００に追加するという要求によって連絡を受ける。ディジタル・コンテンツ・レーベルは、電子ディジタル・コンテンツ・ストア１０３の名前と、クリアリング・ハウス１０５が電子ディジタル・コンテンツ・ストア１０３用のディジタル証書を作成するために必要と思われるその他の情報を提供する。ディジタル証書は、安全なやり方でディジタル・コンテンツ・レーベルに送られ、ディジタル・コンテンツ・レーベルによって電子ディジタル・コンテンツ・ストア１０３に転送される。クリアリング・ハウス１０５は、それが割り当てたディジタル証書のデータベースを維持する。各証書は、バージョン番号、固有の通し番号、サイン・アルゴリズム、発行者の名前（たとえば、クリアリング・ハウス１０５の名前）、その証書が有効と見なされる期間、電子ディジタル・コンテンツ・ストア１０３の名前、電子ディジタル・コンテンツ・ストア１０３の公開キー、クリアリング・ハウス１０５の秘密キーを使用してサインした他の情報すべてのハッシュ・コードを含む。クリアリング・ハウス１０５の公開キー６２１を有するエンティティは、その証書を妥当性検査することができ、その後、証書からの公開キーを使用して妥当性検査可能なシグニチャが付いたＳＣは有効なＳＣであることが保証される。

【０１４９】電子ディジタル・コンテンツ・ストア１０３は、クリアリング・ハウス１０５によって作成されたそのディジタル証書と、ＳＣを処理するために必要なツ

ールをディジタル・コンテンツ・レーベルから受け取った後、エンドユーザが購入可能なコンテンツ１１３の提供を開始することができる。電子ディジタル・コンテンツ・ストア１０３は、その証書とトランザクションＳＣ６４０を含み、そのディジタル・シグニチャ６４３を使用してＳＣにサインする。エンドユーザ装置１０９は、まずディジタル証書撤回リストをチェックし、次にクリアリング・ハウス１０５の公開キー６２１を使用して電子ディジタル・コンテンツ・ストア１０３用のディジタル証書内の情報を検証することにより、電子ディジタル・コンテンツ・ストア１０３がセキュア・ディジタル・コンテンツ電子配布システム１００上でコンテンツ１１３の有効な配布者であることを検証する。ディジタル証書撤回リストはクリアリング・ハウス１０５によって維持される。撤回リストは、クリアリング・ハウス１０５によって作成されるライセンスＳＣ６６０のパーツの１つとして含めることができる。エンドユーザ装置１０９は、電子ディジタル・コンテンツ・ストア１０３のディジタル証書妥当性検査の一部としてそれを使用できるように、エンドユーザ装置１０９上に撤回リストのコピーを保持する。エンドユーザ装置１０９は、ライセンスＳＣ６６０を受け取ると、新しい撤回リストが含まれているかどうかを判定し、含まれている場合にはエンドユーザ装置１０９上のローカル撤回リストが更新される。

【０１５０】Ｂ．権利管理処理

オーダＳＣの分析

エンドユーザがオファーＳＣ６４１を含むトランザクションＳＣ６４０を電子ディジタル・コンテンツ・ストア１０３から受け取った後で、クリアリング・ハウス１０５はそのエンドユーザからオーダＳＣ６５０を受け取る。オーダＳＣ６５０は、コンテンツ１１３とその用途に関連する情報、コンテンツ１１３を販売する電子ディジタル・コンテンツ・ストア１０３に関する情報、コンテンツ１１３を購入するエンドユーザに関する情報を含むパーツからなる。クリアリング・ハウス１０５は、オーダＳＣ６５０内の情報の処理を開始する前に、まずＳＣが実際に有効であり、それが含むデータが決して破壊されていないことを保証するための何らかの処理を実行する。

【０１５１】妥当性検査

クリアリング・ハウス１０５は、ディジタル・シグニチャを検証することにより、オーダＳＣ６５０の妥当性検査を開始し、次にクリアリング・ハウス１０５はオーダＳＣ６５０のパーツの完全性を検証する。ディジタル・シグニチャを妥当性検査するために、まずクリアリング・ハウス１０５は、サイン付きの場合は含まれているサイン・エンティティの公開キー６６１を使用してシグニチャ自体のコンテンツ６３１を暗号化解除する。（サイン・エンティティは、コンテンツ・プロバイダ１０１、電子ディジタル・コンテンツ・ストア１０３、エンドユーザ装置１０９、またはそのいずれかの組合せにすることができるだろう。）次に、クリアリング・ハウス１０５は、ＳＣの連結パーツ・ダイジェストのダイジェストを計算し、それをディジタル・シグニチャの暗号化解除したコンテンツ１１３と比較する。２つの値が一致する場合、ディジタル・シグニチャは有効である。各パーツの完全性を検証するために、クリアリング・ハウス１０５は、そのパーツのダイジェストを計算し、それをＢＯＭ内のダイジェスト値と比較する。クリアリング・ハウス１０５は同じプロセスに従って、オーダＳＣ６５０内に含まれるメタデータおよびオファーＳＣ６４１の各パーツに関するディジタル・シグニチャおよびパーツ完全性を検証する。

【０１５２】また、トランザクションおよびオファーＳＣ６４１のディジタル・シグニチャの検証のプロセスは、電子ディジタル・コンテンツ・ストア１０３がセキュア・ディジタル・コンテンツ電子配布システム１００によって認可されていることも間接的に検証する。これは、クリアリング・ハウス１０５が証書の発行者であることに基づくものである。あるいは、クリアリング・ハウス１０５は、電子ディジタル・コンテンツ・ストア１０３からの公開キーを使用してトランザクションＳＣ６４０およびオファーＳＣ６４１のディジタル・シグニチャを正常に検証できるだろうが、ＳＣにサインしたエンティティが関連の秘密キーの所有権を有する場合に限る。秘密キーの所有権を有するのは電子ディジタル・コンテンツ・ストア１０３だけである。ただし、クリアリング・ハウス１０５は電子ディジタル・コンテンツ・ストア１０３のローカル・データベースを有する必要がないことに留意されたい。というのは、ストアはクリアリング・ハウスの公開キーを使用してトランザクションＳＣ６４０およびオファーＳＣ６４１の公開キーにサインするからである。

【０１５３】次に、エンドユーザが購入するコンテンツ１１３のストア使用条件５１９がメタデータＳＣ６２０に設定された制限の範囲に含まれることを保証するために、その条件がクリアリング・ハウス１０５によって妥当性検査される。メタデータＳＣ６２０がオーダＳＣ６５０内に含まれることを想起されたい。

【０１５４】キー処理

暗号化対称キー６２３およびウォータマーク命令の処理は、オーダＳＣ６５０の信憑性および完全性チェック、電子ディジタル・コンテンツ・ストア１０３の妥当性検査、ストア使用条件５１９の妥当性検査が正常に完了した後で、クリアリング・ハウス１０５によって行われる。オーダＳＣ６５０のメタデータＳＣ６２０部分は通常、クリアリング・ハウス１０５の公開キー６２１を使用して暗号化したキー記述パーツ内に位置する複数の対称キー６２３を有する。対称キー６２３の暗号化は、メタデータＳＣ６２０が作成されたときにコンテンツ・プ

ロバイダ１０１によって行われる。

【０１５５】１つの対称キー６２３はウォータマーク命令を暗号化解除するために使用し、残りの対称キーはコンテンツ１１３および任意の暗号化メタデータを暗号化解除するために使用する。コンテンツ１１３は単一歌曲またはＣＤ上の歌曲の集合全体を表すことができるので、各歌曲ごとに異なる対称キー６２３を使用することができる。ウォータマーク命令はオーダＳＣ６５０のメタデータＳＣ６２０部分内に含まれる。コンテンツ１１３および暗号化メタデータはコンテンツ・ホスト・サイト１１１のコンテンツＳＣ６３０内にある。コンテンツＳＣ６３０内の暗号化コンテンツ１１３およびメタデータ・パーツのＵＲＬおよびパーツ名は、オーダＳＣ６５０のメタデータＳＣ６２０部分のキー記述パーツ内に含まれる。クリアリング・ハウス１０５はその秘密キーを使用して対称キー６２３を暗号化解除し、次にエンドユーザ装置１０９の公開キー６６１を使用してそのそれぞれを暗号化する。エンドユーザ装置１０９の公開キー６６１はオーダＳＣ６５０から取り出される。新しい暗号化対称キー６２３は、クリアリング・ハウス１０５がエンドユーザ装置１０９に返すライセンスＳＣ６６０のキー記述パーツに含まれる。

【０１５６】対称キー６２３の処理時間中、クリアリング・ハウス１０５はウォータマーク命令に変更を加えたいと希望する場合がある。そうである場合、クリアリング・ハウス１０５が対称キー６２３を暗号化解除した後、ウォータマーク命令が変更され、再暗号化される。新しいウォータマーク命令は、エンドユーザ装置１０９に返されるライセンスＳＣ６６０内のパーツの１つとして含まれる。

【０１５７】オーダＳＣ６５０のすべての処理が成功した場合、クリアリング・ハウス１０５はエンドユーザ装置１０９にライセンスＳＣ６６０を返す。エンドユーザ装置１０９はライセンスＳＣ６６０情報を使用してコンテンツＳＣ６３０をダウンロードし、暗号化コンテンツ１１３およびメタデータにアクセスする。また、ウォータマーク命令もエンドユーザ装置１０９によって実行される。

【０１５８】クリアリング・ハウス１０５がオーダＳＣ６５０を正常に処理できない場合、エンドユーザ装置１０９にＨＴＭＬページが返され、そのページがインターネット・ブラウザのウィンドウに表示される。そのＨＴＭＬページは、クリアリング・ハウス１０５がそのトランザクションを処理できなかった理由を示す。

【０１５９】代替実施形態では、ユーザがその販売について設定されたリリース日以前にコンテンツ１１３のコピーを購入した場合、対称キー６２３なしでライセンスＳＣ６６０が返される。対称キー６２３を受け取るためにリリース日以降にライセンスＳＣ６６０がクリアリング・ハウス１０５に返される。一例として、コンテンツ・プロバイダ１０１は、ユーザが新しい歌曲のリリース日以前にその歌曲をダウンロードできるようにし、顧客がコンテンツ・プロバイダ１０１によって設定された日付前にその歌曲をダウンロードしてその歌曲を再生する準備ができるようにする。このため、リリース日に帯域幅およびダウンロード時間に対して不満をなくす必要なしに、リリース日にコンテンツ１１３を直ちにオープンすることができる。

【０１６０】Ｃ．国別固有パラメータ

任意選択で、クリアリング・ハウス１０５は、エンドユーザ装置１０９のドメイン名と、可能であれば、クレジット・カード請求アドレスを使用して、エンドユーザの国別位置を判定する。エンドユーザが在住する国内でコンテンツ１１３の販売に関する何らかの制限がある場合、クリアリング・ハウス１０５は、エンドユーザ装置１０９にライセンスＳＣ６６０を伝送する前に処理中のトランザクションがこれらの制限のいずれにも違反しないことを保証する。また、電子ディジタル・コンテンツ・ストア１０３も、クリアリング・ハウス１０５と同じチェックを実行することにより様々な国へのコンテンツ１１３の配布の管理に関与するものと予想される。クリアリング・ハウス１０５は、コンテンツ・プロバイダ１０１が設定した国別固有規則を電子ディジタル・コンテンツ・ストア１０３が無視する場合にそれが行えるものであればどんなチェックでも実行する。

【０１６１】Ｄ．監査ログおよび追跡

クリアリング・ハウス１０５は、コンテンツ１１３の購入トランザクションおよび報告要求トランザクション中に実行される各動作に関する情報の監査ログ１５０を維持する。この情報は、セキュア・ディジタル・コンテンツ電子配布システム１００の監査、報告書の作成、データ・マイニングなど、様々な目的に使用することができる。

【０１６２】また、クリアリング・ハウス１０５は、電子ディジタル・コンテンツ・ストア１０３用の請求サブシステム１８２において口座残高も維持する。電子ディジタル・コンテンツ・ストア１０３用の価格設定構造は、ディジタル・コンテンツ・レーベルによってクリアリング・ハウス１０５に提供される。この情報は、電子ディジタル・コンテンツ・ストア１０３に課す必要がある現行特価、ボリューム割引、口座残高不足限度のようなものを含むことができる。クリアリング・ハウス１０５は価格設定情報を使用して、電子ディジタル・コンテンツ・ストア１０３の残高を追跡し、コンテンツ・プロバイダ１０１が設定したその残高不足限度を超えないことを保証する。

【０１６３】以下の動作は、通常、クリアリング・ハウス１０５によってログ記録される。

・　ライセンスＳＣ６６０を求めるエンドユーザ装置１０９の要求

・　クリアリング・ハウス１０５が請求を処理する際のクレジット・カード認証番号
・　エンドユーザ装置１０９へのライセンスＳＣ６６０の分散
・　報告を求める要求
・　コンテンツＳＣ６３０およびライセンスＳＣ６６０を受け取り、妥当性検査したというエンドユーザからの通知
【０１６４】以下の情報は、通常、ライセンスＳＣ６６０に関してクリアリング・ハウス１０５によってログ記録される。
・　要求の日付と時刻
・　購入トランザクションの日付と時刻
・　購入する項目のコンテンツＩＤ
・　コンテンツ・プロバイダ１０１の識別名
・　ストア使用条件５１９
・　ウォータマーク命令の変更
・　電子ディジタル・コンテンツ・ストア１０３によって追加されたトランザクションＩＤ５３５
・　電子ディジタル・コンテンツ・ストア１０３の識別名
・　エンドユーザ装置１０９の識別名
・　エンドユーザのクレジット・カード情報（クリアリング・ハウス１０５が請求を処理する場合）
【０１６５】以下の情報は、通常、エンドユーザのクレジット・カード妥当性検査に関してクリアリング・ハウス１０５によってログ記録される。
・　要求の日付と時刻
・　クレジット・カードに請求される金額
・　購入する項目のコンテンツＩＤ
・　電子ディジタル・コンテンツ・ストア１０３によって追加されたトランザクションＩＤ５３５
・　電子ディジタル・コンテンツ・ストア１０３の識別名
・　エンドユーザ装置の識別名
・　エンドユーザのクレジット・カード情報
・　クレジット・カードの決済業者から受け取った認証番号
【０１６６】以下の情報は、通常、ライセンスＳＣ６６０がエンドユーザ装置１０９に送られたときにクリアリング・ハウス１０５によってログ記録される。
・　要求の日付と時刻
・　購入する項目のコンテンツＩＤ
・　コンテンツ・プロバイダ１０１の識別名
・　使用条件５１７
・　電子ディジタル・コンテンツ・ストア１０３によって追加されたトランザクションＩＤ５３５
・　電子ディジタル・コンテンツ・ストア１０３の識別名
・　エンドユーザ装置の識別名
【０１６７】以下の情報は、通常、報告要求が行われたときにログ記録される。
・　要求の日付と時刻
・　報告が送られた日付と時刻
・　要求された報告のタイプ
・　報告書を作成するために使用するパラメータ
・　報告を要求したエンティティの識別子
【０１６８】Ｅ．結果の報告
報告書は、クリアリング・ハウス１０５がエンドユーザの購入トランザクション中にログ記録した情報を使用して、クリアリング・ハウス１０５によって作成される。コンテンツ・プロバイダ１０１と電子ディジタル・コンテンツ・ストア１０３は、クリアリング・ハウス１０５によってログ記録された情報とそれ自身のトランザクション・データベースとの調停を行えるように、支払検証インタフェース１８３を介してクリアリング・ハウス１０５からトランザクション報告を要求することができる。また、クリアリング・ハウス１０５は、コンテンツ・プロバイダ１０１および電子ディジタル・コンテンツ・ストア１０３に対して定期的な報告を行うこともできる。
【０１６９】クリアリング・ハウス１０５は、コンテンツ・プロバイダ１０１および電子ディジタル・コンテンツ・ストア１０３が報告を要求し受け取れるようにする、安全な電子インタフェースを定義する。報告要求ＳＣは、要求を行ったエンティティにクリアリング・ハウス１０５が割り当てた証書を含む。クリアリング・ハウス１０５はその証書とＳＣのディジタル・シグニチャを使用して、その要求が認可エンティティから出されたことを検証する。また、この要求は、期間など、報告の範囲を定義するパラメータも含む。クリアリング・ハウス１０５は要求パラメータを妥当性検査し、要求側がそれに関して有することが許された情報だけを受け取れることを保証する。
【０１７０】報告要求ＳＣが真正かつ有効であるとクリアリング・ハウス１０５が判断した場合、クリアリング・ハウス１０５は報告書を作成し、要求を出したエンティティに送るべき報告ＳＣにそれをパックする。報告書によっては、要求を受け取ったときに直ちに送ることができるように、定義された時間間隔で自動的に作成され、クリアリング・ハウス１０５に記憶される場合もある。報告書に含まれるデータのフォーマットは本書の今後のバージョンで定義される。
【０１７１】Ｆ．請求および支払検証
コンテンツ１１３の請求は、クリアリング・ハウス１０５または電子ディジタル・コンテンツ・ストア１０３のいずれかによって処理することができる。クリアリング・ハウス１０５が電子コンテンツ１１３の請求を処理する場合、電子ディジタル・コンテンツ・ストア１０３はエンドユーザのオーダを分離して電子商品にし、適用可

能であれば、物理的商品にする。次に、電子ディジタル・コンテンツ・ストア１０３は、エンドユーザの請求情報を含むトランザクションと、認証する必要がある合計金額についてクリアリング・ハウス１０５に通知する。クリアリング・ハウス１０５はエンドユーザのクレジット・カードを認証し、電子ディジタル・コンテンツ・ストア１０３に通知を返す。クリアリング・ハウス１０５がエンドユーザのクレジット・カードを認証すると同時に、電子ディジタル・コンテンツ・ストア１０３は購入する物理的商品についてエンドユーザのクレジット・カードに請求することができる。エンドユーザ装置１０９が各電子項目をダウンロードした後、クリアリング・ハウス１０５は、エンドユーザのクレジット・カードに請求できるように通知を受ける。これは、エンドユーザ装置１０９での使用のためにコンテンツ１１３を使用可能にする前に、エンドユーザ装置１０９による最後のステップとして行われる。

【０１７２】電子ディジタル・コンテンツ・ストア１０３が電子コンテンツ１１３の請求を処理する場合、クリアリング・ハウス１０５は、エンドユーザ装置１０９がクリアリング・ハウス１０５にオーダＳＣ６５０を送るまでトランザクションに関する通知を受け取らない。クリアリング・ハウス１０５は、各電子項目をダウンロードした後でエンドユーザ装置１０９から通知を受ける。クリアリング・ハウス１０５は、通知を受けると、電子ディジタル・コンテンツ・ストア１０３がエンドユーザのクレジット・カードに請求できるように電子ディジタル・コンテンツ・ストア１０３に通知を送る。

【０１７３】Ｇ．再伝送

セキュア・ディジタル・コンテンツ電子配布システム１００は、コンテンツ１１３の再伝送を処理する能力を提供する。これは、通常、顧客サービス・インタフェース１８４によって実行される。電子ディジタル・コンテンツ・ストア１０３は、再伝送を開始するためにエンドユーザが段階的に実行できるユーザ・インタフェースを提供する。エンドユーザは、コンテンツ１１３の再伝送を要求するためにコンテンツ１１３の項目を購入した電子ディジタル・コンテンツ・ストア１０３のサイトへ移動する。

【０１７４】コンテンツ１１３の再伝送は、コンテンツ１１３がダウンロードできなかったかまたはダウンロードしたコンテンツ１１３が使用不能であるためにエンドユーザが前に購入したコンテンツ１１３の項目の新しいコピーを要求したときに行われる。電子ディジタル・コンテンツ・ストア１０３は、コンテンツ１１３の再伝送を実行する資格がエンドユーザに与えられているかどうかを判定する。再伝送の資格がエンドユーザに与えられている場合、電子ディジタル・コンテンツ・ストア１０３は、再伝送するコンテンツ１１３の項目のオファーＳＣ６４１を含むトランザクションＳＣ６４０を構築する。トランザクションＳＣ６４０はエンドユーザ装置１０９に送られ、購入トランザクションの場合と同一のステップがエンドユーザによって行われる。エンドユーザ装置１０９が再伝送されるコンテンツ１１３の項目用のキー・ライブラリ内にスクランブル済みキーを有する場合、トランザクションＳＣ６４０は、スクランブル済みキーを削除するようエンドユーザ装置１０９に指示する情報を含む。

【０１７５】クリアリング・ハウス１０５がコンテンツ１１３の購入の金融決済を処理する場合、電子ディジタル・コンテンツ・ストア１０３は、オーダＳＣ６５０でクリアリング・ハウス１０５に転送されるフラグをトランザクションＳＣ６４０に含める。クリアリング・ハウス１０５は、オーダＳＣ６５０内のフラグを解釈し、コンテンツ１１３の購入についてエンドユーザに請求せずにトランザクションを続行する。

【０１７６】VIII．コンテンツ・プロバイダ

Ａ．概要

セキュア・ディジタル・コンテンツ電子配布システム１００におけるコンテンツ・プロバイダ１０１は、コンテンツ１１３に対する権利を所有するディジタル・コンテンツ・レーベルまたはエンティティである。コンテンツ・プロバイダ１０１の役割は、コンテンツ１１３を配布用に作成し、電子ディジタル・コンテンツ・ストア１０３またはコンテンツ１１３のダウンロード可能な電子バージョンの小売業者に対しコンテンツ１１３に関する情報を使用可能にすることである。コンテンツ・プロバイダ１０１に対し最大限のセキュリティと権利制御を提供するため、コンテンツ１１３がコンテンツ・プロバイダ１０１のドメインを去るときにそれが安全であり、無許可当事者によって決して公表されずアクセス不能になるように、コンテンツ・プロバイダがその構内で自分のコンテンツ１１３を作成してＳＣ内に確実にパッケージ化できるようにするための一連のツールが用意されている。このため、コンテンツ１１３は、ハッカまたは無許可当事者に対して公表される恐れなしに、インターネットなどの安全ではないネットワークのいたるところに自由に配布することができる。

【０１７７】コンテンツ・プロバイダ１０１用のツールの最終的な目標は、１つの歌曲または一連の歌曲などのコンテンツ１１３を作成してコンテンツＳＣ６３０内にパッケージ化することと、その歌曲を説明する情報、その歌曲の承認済み用途（コンテンツの使用条件５１７）、その歌曲に関するプロモーション情報をメタデータＳＣ６２０内にパッケージ化することである。これを実施するため、以下の１組のツールが用意されている。

・　ワーク・フロー・マネージャ１５４　－　処理活動をスケジューリングし、プロセス同士の必須の同期を管理する。

・　コンテンツ処理ツール１５５　－　ウォータマー

ク、前処理（オーディオ例の場合、必須の等化、強弱の変化の調節、再サンプリング）、コード化、圧縮を含む、コンテンツ１１３のファイル作成を制御するためのツールの集合。

・　メタデータ同化入力ツール１６１　－　コンテンツ・プロバイダのデータベース１６０または第三者のデータベースあるいはデータ・インポート・ファイルからもしくはオペレータの対話によりコンテンツ１１３の記述情報を収集するために使用するツールの集合であって、コンテンツの使用条件５１７を指定するための手段を提供する。また、ＣＤまたはＤＤＰファイル用のディジタル・オーディオ・コンテンツなどのコンテンツを取り込むかまたは抽出するためのインタフェースも提供する。

・　品質管理ツールは、作成したコンテンツおよびメタデータのプリビューを可能にする。メタデータに加える必要がある訂正またはさらに処理するためのコンテンツの再提示を行うことができる。

・　ＳＣパッカ・ツール１５２　－　すべてのコンテンツ１１３および情報を暗号化してパッケージ化し、ＳＣパッカを呼び出してＳＣ内にパックする。

・　コンテンツ分散ツール（図示せず）　－　コンテンツ・ホスト・サイト１１１および電子ディジタル・コンテンツ・ストア１０３などの指定の配布センターにＳＣを分散する。

・　コンテンツ・プロモーション・ウェブ・サイト１５６　－　認可電子ディジタル・コンテンツ・ストア１０３によるダウンロードのためにメタデータＳＣ６２０および任意選択で追加のプロモーション素材を記憶する。

【０１７８】Ｂ．ワーク・フロー・マネージャ１５４

このツールの目的は、コンテンツ１１３の処理活動をスケジューリングし、追跡し、管理することである。このアプリケーションにより、マルチユーザ・アクセスが可能になると同時に、コンテンツ・プロバイダ１０１のイントラネットまたはエクストラネット内のリモート位置からコンテンツ１１３のスケジューリングおよび情況チェックが可能になる。また、この設計は協調処理も可能にし、その場合、複数の個人がコンテンツ１１３の複数のピースについて並行して作業することができ、それぞれ異なる個人に特定の責任を割り当てることができ、このような個人を世界中に分散させることができる。

【０１７９】次に図１１に移行すると、図１０に対応するワーク・フロー・マネージャ１５４の主要プロセスを示すブロック図である。図１１の主要プロセスは、この項で説明するツールによって提供されるコンテンツ１１３処理機能を要約したものである。ワーク・フロー・マネージャ１５４は、これらのプロセスにジョブを供給し、その現行プロセスの完了時に次の必須プロセスにジョブを向けることを担当する。これは、以下の動作を実行するために各処理ツールが呼び出す一連のアプリケーション・プログラミング・インタフェース（ＡＰＩ）により実施される。

・　処理すべき次のジョブを取り出す。

・　プロセスの正常終了を示す。

・　プロセスの終了失敗とその失敗の理由を示す。

・　プロセスの暫定状況を示す（従属プロセスの部分完了のみを必要とするプロセスの開始を可能にするため）

・　指定のプロセスにとって使用可能なコメントを製品に追加する。

【０１８０】ワーク・フロー・マネージャ１５４はユーザ・インタフェースも有し、一例としてワーク・フロー・マネージャ・ユーザ・インタフェース７００を図１０に示すが、これは以下の機能を提供する。

・　処理の様々な段階で割り当てて実行すべきデフォルト値および条件の指定を可能にするための構成パネル

・　ワーク・フロー規則および自動処理フローのカストマイズ

・　ジョブ・スケジューリング

・　状況照会および報告

・　１つまたは複数のプロセスに関連するジョブのコメントまたは命令を追加すること

・　ジョブ管理（すなわち、中断、解放、除去、優先順位（処理の順序）変更）

【０１８１】各プロセスは、それに関連する待ち行列をワーク・フロー・マネージャ１５４によって管理させる。いずれのプロセスもワーク・フロー・マネージャ１５４からジョブを要求すると、その結果、ワーク・フロー・マネージャ１５４は、その関連待ち行列内に現在いかなるジョブも存在しない場合にプロセス（ツール）を中断して待ち状態にするか、それぞれのプロセスを実行するために必要なジョブに関するすべての情報をプロセスに返す。プロセスを中断して待ち状態にした場合、ワーク・フロー・マネージャ１５４によってその待ち行列にジョブが置かれると、そのプロセスが処理を再開する。

【０１８２】また、ワーク・フロー・マネージャ１５４は、１組の定義済み規則に基づいて処理のフローまたは順序も管理する。これらの規則は、コンテンツ・プロバイダ１０１が特殊処理要件を有するかまたは特定のデフォルト規則を構成する場合に、そのプロバイダによってカストマイズすることができる。あるプロセスがその割当てタスクの完了を報告すると、そのプロセスはワーク・フロー・マネージャ１５４にこの状況を通知し、ワーク・フロー・マネージャ１５４は定義済み規則に基づいて次にそのジョブがどの待ち行列に置かれるかを決定する。

【０１８３】プログラミングＡＰＩによるかまたはワーク・フロー・マネージャ・ユーザ・インタフェース７００またはプロセッサ・インタフェースにより手動で、いずれかの処理ステップで特殊処理命令または通知を示すコメントも製品に付加することができる。

【０１８４】ワーク・フロー・マネージャ１５４におけるプロセスは、好ましい実施形態ではJavaで実現されるが、Ｃ／Ｃ＋＋、アセンブラ、それと同等のものなどのその他のプログラミング言語も使用することができる。ただし、ワーク・フロー・マネージャ１５４に関して後述するプロセスは様々なハードウェアおよびソフトウェア・プラットフォーム上で実行できることに留意されたい。完全なシステムとしてまたはその構成プロセスのいずれかとしてのワーク・フロー・マネージャ１５４は、ウェブなどの電子配布またはフロッピー（登録商標）・ディスケット、ＣＤ－ＲＯＭ、取外し可能ハード・ディスク・ドライブを含みかつこれに限定されないコンピュータ可読媒体に入れてアプリケーション・プログラムとして配布することができる。

【０１８５】次に図１１に移行すると、図１０に対応するワーク・フロー・マネージャ１５４の主要プロセスを示すブロック図である。以下の各項では、各プロセスについて要約し、各プロセスが必要とする情報またはアクションについて説明する。

【０１８６】１．製品待受けアクション／情報プロセス８０１

そのプロセスが必要とするすべての情報が使用可能になり、そのジョブがすべての従属処理をすでに正常に完了していると、特定のプロセス待ち行列にジョブが置かれる。ワーク・フロー・マネージャ１５４には、情報の欠落またはその後の処理を妨げるような障害のために、現在、処理に使用可能ではないジョブを保持するために使用する特殊待ち行列が存在する。これらのジョブは、製品待受けアクション／情報プロセス８０１の待ち行列に置かれる。この待ち行列内の各ジョブは、それが応対するアクションまたは情報、このジョブに作用した最後のプロセス、欠落情報または追加の情報が提供されるかまたは必須アクションが正常に完了したときにこのジョブが待ち行列化される次のプロセスを示すために関連状況を有する。

【０１８７】いずれかのプロセスが完了すると、ワーク・フロー・マネージャ１５４はこの待ち行列をチェックし、この待ち行列内のいずれかのジョブがこのプロセス（アクション）の完了またはこのプロセスによって提供される情報を待っているかどうかを判定する。そうである場合、そのジョブは適切なプロセス待ち行列に待ち行列化される。

【０１８８】２．新コンテンツ要求プロセス８０２

コンテンツ・プロバイダ１０１は、それが販売し、電子的に送達したいと希望する製品（たとえば、製品は１曲の歌曲である場合もあれば、複数歌曲の集合である場合もある）を決定する。ワーク・フロー・マネージャ１５４の初期機能は、オペレータがこのような製品を識別し、それを新コンテンツ要求プロセス８０２の待ち行列に置くことができるようにすることである。コンテンツ・プロバイダ１０１は、製品選択インタフェースでどの情報が要求されるかを構成オプションにより指定することができる。その製品を明確に識別するために十分な情報が入力される。任意選択で、メタデータ収集と並行してオーディオ処理フェーズを開始するために必要な情報の手動入力を要求するために、追加のフィールドを含めることもできる。手動で提供されない場合、任意選択で、自動メタデータ収集プロセス８０３のようにメタデータ処理の第１の段階で得られるコンテンツ・プロバイダのデータベース１６０からまたはデフォルト構成設定からこの情報を取り出すことができる。コンテンツ・プロバイダのデータベース１６０におけるコンテンツ１１３の構成および諸機能によってコンテンツ選択プロセスが決定される。

【０１８９】コンテンツ・プロバイダ１０１のデータベース１６０への照会を実行するために必要な必須情報が指定された場合、そのジョブは自動メタデータ収集プロセス８０３によって処理される。音楽の実施形態では、オーディオ処理のためにその製品を適切にスケジューリングするために、製品のジャンルと所望の圧縮レベルならびにオーディオＰＣＭまたはＷＡＶファイル名が指定される。この情報は、製品選択プロセスの一部として入力するかまたはカストマイズ照会インタフェースまたはウェブ・ブラウザ機能により選択することができる。この情報を指定すると、コンテンツ処理のために製品をスケジューリングすることができる。

【０１９０】製品選択ユーザ・インタフェースは、処理のために製品をリリースできるかどうかまたは追加の情報入力までそれを保持するかどうかをオペレータが指定できるようにするオプションを提供する。保持する場合、ジョブは新コンテンツ要求プロセス８０２の待ち行列に追加され、データ入力を完了するかまたは処理のためにその製品をリリースするかあるいはその両方のために次のアクションを待つ。製品がリリースされると、ワーク・フロー・マネージャ１５４は指定した情報を評価し、どのプロセスがそのジョブに渡される状態になっているかを判定する。

【０１９１】コンテンツ・プロバイダ１０１のデータベース１６０に対する自動照会を可能にするために十分な情報が提供された場合、そのジョブは自動メタデータ収集プロセス８０３のために待ち行列化される。自動メタデータ収集プロセス８０３のためにデータベース・マッピング・テーブルが構成されていない場合、そのジョブは手動メタデータ入力プロセス８０４のために待ち行列化される（データベース・マッピング・テーブルに関する詳細については自動メタデータ収集プロセス８０３の項を参照）。

【０１９２】オーディオ処理のための必須一般情報とウォータマークに必要な特殊情報が指定された場合、そのジョブはウォータマーク・プロセス８０８（コンテンツ

処理の第１のフェーズ）のために待ち行列化される。ジョブがリリースされたときに必須情報のいずれかが欠落している場合、そのジョブは、欠落した情報を示す状況とともに、製品待受けアクション／情報プロセス８０１の待ち行列に待ち行列化される。

【０１９３】たとえば、コンテンツ１１３がオーディオであり、ＰＣＭまたはＷＡＶファイルが欠落しているようなコンテンツ１１３のファイル名をその状況が示す場合、これは、取込み（またはディジタル媒体からのディジタル抽出）が必要であることを示す場合もある。オーディオ処理機能では、歌曲ファイルは標準のファイル・システム・インタフェースによりアクセス可能でなければならない。歌曲が外部媒体またはオーディオ処理ツールが直接アクセスできないファイル・システム上に位置する場合、そのファイルはまずアクセス可能なファイル・システムにコピーされる。歌曲がディジタル・フォーマットになっているがＣＤまたはディジタル・テープ上にある場合、その歌曲はオーディオ処理ツールにとってアクセス可能なファイル・システムに抽出される。そのファイルがアクセス可能になると、ウォータマークに必要な他のすべての情報もすでに指定されていると想定し、ワーク・フロー・マネージャ・ユーザ・インタフェース７００を使用して、それをウォータマーク・プロセスにリリースできるようにそのジョブ用のパスおよびファイル名を指定または選択する。

【０１９４】３．自動メタデータ収集プロセス８０３

自動メタデータ収集プロセス８０３は、製品情報のうちのできるだけ多くを自動的に入手しようと試みて、コンテンツ・プロバイダ１０１のデータベース１６０またはデータがインポートされたステージング・データベースへの一連の照会を実行する。自動メタデータ収集プロセス８０３では、その待ち行列に項目を置けるようになる前に以下の情報を必要とする。・　コンテンツ・プロバイダ１０１のデータベース１６０への照会を生成するために十分な情報を備えたデータベース・マッピング・テーブル

・　照会を実行するために必要な製品情報

・　製品を明確に定義するために十分な製品情報

【０１９５】このコンテンツ１１３を処理するために必要な情報を入手するために、コンテンツ・プロバイダ１０１のデータベース１６０への自動照会が実行される。たとえば、コンテンツ１１３が音楽である場合、この照会を実行するために必要な情報はアルバム名にすることもできるが、ＵＰＣであるかまたはコンテンツ・プロバイダ１０１によって定義された特定のアルバムまたは選択ＩＤにすることもできる。入手すべき情報の一部は必須のものとして指定される（詳細については自動メタデータ収集プロセス８０３に関する項を参照）。すべての必須情報を入手した場合、次にそのジョブは使用条件プロセス８０５のために待ち行列化される。いずれかの必須情報が欠落している場合、その歌曲は手動メタデータ入力プロセス８０４のために待ち行列化される。製品待受けアクション／情報プロセス８０１の待ち行列内のいずれかのジョブがこのステップで入手した情報のいずれかを待っている場合、それがもはやこの情報を待っていないことを示すためにジョブ状況が更新される。そのジョブがもはや未処理の要件を持っていない場合、それは次の定義済み待ち行列に待ち行列化される。

【０１９６】４．手動メタデータ入力プロセス８０４

手動メタデータ入力プロセス８０４は、オペレータが欠落情報を入力するための手段を提供する。これには、依存関係はない。すべての必須情報が指定されると、そのジョブは使用条件プロセス８０５のために待ち行列化される。

【０１９７】５．使用条件プロセス８０５

使用条件プロセス８０５は、製品用途および制限の指定を可能にするものである。使用条件プロセス８０５は何らかのメタデータを必要とする場合がある。使用条件の指定が完了すると、そのジョブは、監視付きリリース・プロセス８０６オプションがすでに要求されたかまたはワーク・フロー・マネージャ１５４の規則にデフォルトとして構成されるまで、メタデータＳＣ作成プロセス８０７のために待ち行列化される資格が与えられる。その場合、そのジョブは監視付きリリース・プロセス８０６のために待ち行列化される。メタデータＳＣ作成プロセス８０７に待ち行列化する前に、ワーク・フロー・マネージャ１５４はまず、そのプロセスに関するすべての依存関係が満たされていることを保証する（以下参照）。そうではない場合、そのジョブは製品待受けアクション／情報プロセス８０１に待ち行列化される。

【０１９８】６．監視付きリリース・プロセス８０６

監視付きリリース・プロセス８０６は、ディジタル・コンテンツ製品について指定された情報の品質チェックおよび妥当性検査を可能にする。これには、いかなる依存関係もない。この製品の処理のいずれかの段階でそのジョブに事前に付加したコメントはスーパバイザが検討し、適切なアクションを講じることができる。すべての情報およびコメントの検討後、スーパバイザは以下のオプションを有する。

・　リリースを承認し、メタデータＳＣ作成プロセス８０７のためにその製品を待ち行列化する。

・　情報の変更または追加あるいはその両方を行い、メタデータＳＣ作成プロセス８０７のためにその製品を待ち行列化する。

・　そのジョブにコメントを追加し、手動メタデータ入力プロセス８０４のために再待ち行列化する。

・　コメントを追加し、製品待受けアクション／情報プロセス８０１のための待ち行列にそのジョブを待ち行列化する。

【０１９９】７．メタデータＳＣ作成プロセス８０７

メタデータＳＣ作成プロセス８０７は、上記で収集したすべての情報ならびにメタデータＳＣ６２０に必要なその他の情報をまとめて収集し、ＳＣパッカ・プロセスを呼び出してメタデータＳＣ６２０を作成する。このツールは入力として以下のものを必要とする。

・　必須メタデータ
・　使用条件
・　この製品のためにすべての品質レベルの暗号化段階で使用する暗号化キー

【０２００】この最後の依存関係では、メタデータＳＣ６２０を作成する前に関連オーディオ・オブジェクトがオーディオ処理フェーズを完了していなければならない。メタデータＳＣ作成プロセス８０７が完了すると、そのジョブは、定義済みワーク・フロー規則に基づいて最終品質保証プロセス８１３またはコンテンツ分散プロセス８１４のいずれかのための待ち行列に待ち行列化される。

【０２０１】８．ウォータマーク・プロセス８０８

ウォータマーク・プロセス８０８は、著作権およびその他の情報をコンテンツ１１３に追加するものである。コンテンツ１１３が歌曲である実施形態の場合、このツールは入力として以下のものを必要とする。

・　歌曲ファイル名（アルバムの場合は複数のファイル名）
・　ウォータマーク命令
・　ウォータマーク・パラメータ（ウォータマークに含める情報）

【０２０２】ウォータマーク・プロセス８０８が完了すると、そのジョブは、その必須入力が使用可能である場合には前処理圧縮プロセス８０９のために待ち行列化され、そうではない場合には製品待受けアクション／情報プロセス８０１に待ち行列化される。

【０２０３】９．前処理圧縮プロセス８０９

前処理圧縮プロセス８０９は、指定の圧縮レベルに応じてコンテンツ１１３をコード化し、どの必須前処理も先に実行する。この待ち行列に１つのジョブを待ち行列化すると、実際には、複数の待ち行列項目が作成される。所望の製品の各圧縮レベルごとに１つのジョブが作成される。コード化プロセスは、複数のシステムで並行して実行することができる。このツールは以下の入力を必要とする。

・　ウォータマーク付きコンテンツ・ファイル名（コンテンツ１１３がアルバムの場合は複数のファイル名）
・　製品の品質レベル（事前構成可能）
・　圧縮アルゴリズム（事前構成可能）
・　製品ジャンル（プリプロセッサが必要とする場合）

【０２０４】コード化プロセスが完了すると、そのジョブは、ワーク・フロー規則によって構成された場合にはコンテンツ品質管理プロセス８１０に待ち行列化される。そうではない場合には、ジョブは暗号化プロセス８１１のために待ち行列化される。

【０２０５】オーディオなどのコンテンツ１１３のうち、すでに処理されたコンテンツの割合を表示するための方法またはコンテンツ１１３のうち、すでにコード化されたコンテンツの量を選択したコンテンツ１１３の選択内容全体のうちの割合として示すための方法をコード化ツールの第三者プロバイダが提供しない場合、図１１のコンテンツ前処理圧縮ツール用のディジタル・コンテンツのコード化速度を決定するための方法の流れ図１１００を図１４に示す。この方法は、ステップ１１０１における所望のコード化アルゴリズムおよびビット伝送速度の選択から始まる。次に、ステップ１１０２では、このアルゴリズムおよびコード化速度が前に計算された速度係数を有するかどうかを判定するための照会を行う。この速度係数は、特定のコード化アルゴリズムおよび特定のビット伝送速度の場合の圧縮速度を決定するために使用する係数である。前に計算された速度係数が一切記憶されていない場合、所定量の時間の間、コンテンツ１１３のサンプルをコード化する。好ましい実施形態では所定の期間は数秒である。所定の期間用のこのコード化速度を使用して、新しい速度係数ＲNEWを計算する。ステップ１１０８では、時間の量およびコード化したコンテンツ１１３の量を把握して、ＲNEW＝（コード化したディジタル・コンテンツの長さ）／（時間の量）として新しい速度係数ＲNEWを計算する。ステップ１１０９では、コンテンツ１１３をコード化し、前に計算された速度係数ＲNEWを使用してコード化状況を表示する。次に、将来、このコード化アルゴリズムおよびコード化ビット伝送速度に使用するために、ステップ１１０７でこのコード化速度係数ＲNEWを記憶する。ステップ１１０３で選択したアルゴリズムが前に計算された速度係数ＲSTOREDを有する場合、ステップ１１０４でコンテンツ１１３をコード化し、前に計算された速度係数ＲSTOREDを使用して経過を表示する。その間に、ステップ１１０５でこの選択したアルゴリズムおよびビット伝送速度について、現行速度係数Ｒcurrentを計算する。ステップ１１０６では、この現行速度係数Ｒcurrentを使用して、記憶した速度係数をＲNEW＝（ＲSTORED＋ＲCURRENT）の平均として更新する。速度係数の反復更新により、その後、特定のコード化アルゴリズムおよびビット伝送速度に使用するたびに、コード化速度の決定がますます正確なものになりうる。ステップ１１０７では、今後の使用のために新しい速度ＲNEWを記憶する。現行速度係数Ｒcurrentが所与の範囲またはしきい値分だけ前に記憶された速度係数ＲSTOREDの範囲を超える場合、ＲSTOREDの更新を行わなくてもよい。

【０２０６】次に、コード化状況の表示を提示することができる。コード化状況は、現行コード化速度とともに、コード化速度およびコンテンツ１１３用のファイルの全長に基づいて経過バーとして表示される全コンテン

ツ１１３の割合の表示を含む。また、コード化状況は、コード化のための残り時間も含むことができる。コード化のための残り時間は、計算されたコード化速度RCURRENTをコンテンツ１１３用のファイルの全長で割ることによって計算することができる。コード化状況は、呼出しプロセスを呼び出すことができる他のプログラムに転送することができる。このことによって、コード化に対する監視プログラムまたはコード化時の共依存プログラムが操作され、かつ、より効率よく処理するためにバッチ処理されることを促進できる。ただし、代替実施形態では、コード化がウォータマーク付けのステップを含む可能性があることに留意されたい。

【０２０７】１０．コンテンツ品質管理プロセス８１０

コンテンツ品質管理プロセス８１０は、機能の点で監視付きリリース・プロセス８０６と同様のものである。これは、誰かがこれまでに実行されたコンテンツ処理の品質を妥当性検査できるようにする任意選択ステップである。これは、ウォータマーク・プロセス８０８の完了および前処理圧縮プロセス８０９のコード化部分以外にいかなる依存関係も持っていない。コンテンツ品質管理プロセス８１０が完了すると、以下のオプションが使用可能になる。

・　そのジョブをリリースし、暗号化プロセス８１１のために待ち行列化することができる。

・　コメントを付加し、１つまたは複数のジョブを前処理圧縮プロセス８０９のために再待ち行列化することができる。

【０２０８】最後のオプションでは、コンテンツ品質管理プロセス８１０の後まで歌曲ファイルの未コード化ウォータマーク付きバージョンが引き続き使用可能でなければならない。

【０２０９】１１．暗号化プロセス８１１

暗号化プロセス８１１は、適切なセキュア・ディジタル・コンテンツ電子配布権利管理機能を呼び出して、ウォータマーク付き／コード化歌曲ファイルのそれぞれを暗号化する。このプロセスは、他のすべてのオーディオ処理の完了以外にいかなる依存関係も持っていない。暗号化プロセス８１１のプロセスが完了すると、そのジョブはコンテンツＳＣ作成プロセス８１２のために待ち行列化される。

【０２１０】１２．コンテンツＳＣ作成プロセス８１２

コンテンツＳＣ作成プロセス８１２のプロセスでは、何らかのメタデータ・ファイルをコンテンツＳＣ６３０に含めなければならない場合がある。コンテンツ１１３以外のファイルが必要な場合、そのファイルを収集し、ＳＣパッカ・プロセスを呼び出して、作成したコンテンツ１１３（たとえば、歌曲）の各圧縮レベルごとにコンテンツＳＣ６３０を作成する。コンテンツＳＣ作成プロセス８１２が完了すると、その歌曲は、定義済みワーク・フロー規則に基づいて最終品質保証プロセス８１３またはコンテンツ分散プロセス８１４のいずれかに待ち行列化される。

【０２１１】１３．最終品質保証プロセス８１３

最終品質保証プロセス８１３は、関連メタデータとコンテンツＳＣ６３０との相互参照チェックにより、両者が正しく一致し、そこに含まれるすべての情報およびコンテンツ１１３が正しいものであることを検証できるようにする任意選択ステップである。最終品質保証プロセス８１３が完了すると、そのジョブはコンテンツ分散プロセス８１４のために待ち行列化される。問題が見つかった場合、ほとんどの場合、そのジョブは失敗した段階に再待ち行列化しなければならない。製品は、問題を訂正するために必要な再処理に加え、再暗号化および再パックを経なければならないので、この段階での手直しは非常に高価なものになる。従来の保証段階を使用して、コンテンツ１１３の品質および情報の正確さと完璧さを保証することを大いに推奨する。

【０２１２】１４．コンテンツ分散プロセス８１４

コンテンツ分散プロセス８１４のプロセスは、適切なホスト・サイトへのＳＣの転送を担当する。ＳＣの正常転送後、ジョブ完了状況がログ記録され、そのジョブが待ち行列から削除される。ＳＣの転送時に問題が発生した場合、定義した回数の試行後に、そのジョブは、ワーク・フロー・マネージャ・ツール１５４において、検出されたエラーとともに、失敗したことを示すフラグが付けられる。

【０２１３】１５．ワーク・フロー規則

図１１に関するワーク・フロー規則は、以下のように３つの主要システムで機能する。

Ａ：ワーク・フロー・マネージャ・ツール１５４

１．新コンテンツ要求プロセス８０２

２．製品待受けアクション／情報プロセス８０１

３．最終品質保証プロセス８１３

４．コンテンツ分散（および通知）プロセス８１４

Ｂ：メタデータ同化入力ツール１６１

１．自動メタデータ収集プロセス８０３

２．手動メタデータ入力プロセス８０４

３．監視付きリリース・プロセス８０６

４．メタデータＳＣ作成プロセス８０７

Ｃ：コンテンツ処理ツール１５５

１．ウォータマーク・プロセス８０８（著作権データを必要とする）

２．前処理圧縮プロセス８０９

３．コンテンツ品質管理プロセス８１０

４．暗号化ツール８１１

５．コンテンツＳＣ作成プロセス８１２

【０２１４】ワーク・フロー

コンテンツ１１３選択オペレータは新しい製品を入力し、Ａ１（新コンテンツ要求プロセス８０２）への待ち行列化に取りかかる。

Ａ１：コンテンツ１１３選択オペレータがそれをワーク・フロー・マネージャ・ツール１５４にリリースすると、それはＢ１（自動メタデータ収集プロセス８０３）に待ち行列化される
Ａ２：ステップＢ１（自動メタデータ収集プロセス８０３）からまたはステップＢ２（手動メタデータ入力プロセス８０４）からまたはステップＢ３（監視付きリリース・プロセス８０６）から先行ステップ（メタデータＳＣ作成プロセス８０７）への途上［暗号化キーを必要とする］先行ステップ（メタデータＳＣ作成プロセス８０７）からステップＡ３（最終品質保証プロセス８１３）またはステップＡ４（コンテンツ分散プロセス８１４）への途上［コンテンツＳＣ６３０を必要とする］ステップＣ１（ウォータマーク・プロセス８０８）からステップＣ２（前処理圧縮プロセス８０９）への途上［前処理圧縮プロセス８０９用のメタデータを必要とする］ステップＣ４（暗号化プロセス８１１）からステップＣ５（コンテンツＳＣ作成プロセス８１２）への途上［コンテンツＳＣ６３０パッキング用のメタデータを必要とする］ステップＣ５（コンテンツＳＣ作成プロセス８１２）からステップＡ３（最終品質保証プロセス８１３）またはステップＡ４（コンテンツ分散プロセス８１４）への途上［メタデータＳＣ６２０を必要とする］
Ａ３：ステップＡ３（最終品質保証プロセス８１３）後に待ち行列Ｂ２（手動メタデータ入力プロセス８０４）上に置くかまたは待ち行列Ｂ３（監視付きリリース・プロセス８０６）上に置くかまたは品質保証オペレータが要求する待ち行列内に入れる
Ａ４：ステップＡ４（コンテンツ分散プロセス８１４）後にこの製品についてワーク・フロー・マネージャ・ツール１５４が実行される
Ｂ１：ステップＢ１（自動メタデータ収集プロセス８０３）後にステップＣ１（ウォータマーク・プロセス８０８）に必要なメタデータが存在する場合、この製品を表す項目を待ち行列Ｃ１上に置く（以下の論理も実行する）１ーいずれかの必須メタデータが欠落しているかまたは２ー手動メタデータ・プロバイダに向けられたコメントが存在する場合、その製品を待ち行列Ｂ２（手動メタデータ入力プロセス８０４）上にも置くあるいはこの製品について監視付きリリースが要求された場合、その製品を待ち行列Ｂ３（監視付きリリース・プロセス８０６）上に置くあるいはその製品が要求されたすべての品質レベルについてコンテンツ処理ツール１５５からのすべての情報を有する場合、その製品を先行待ち行列（メタデータＳＣ作成プロセス８０７）上に置くあるいは暗号化キーを必要とすることを示すフラグをその製品に付け、その製品を待ち行列Ａ２（製品待受けアクション／情報プロセス８０１）上に置く
Ｂ２：ステップＢ２（手動メタデータ入力プロセス８０４）中にステップＣ１（ウォータマーク・プロセス８０８）が実行されておらず、しかもステップＣ１に必要なメタデータが存在する場合、この製品を表す項目を待ち行列Ｃ１上に置く（以下の論理も実行する）ステップＣ２（前処理圧縮プロセス８０９）に必要なメタデータが提供されたばかりである場合（以下の論理も実行する）メタデータ同化入力ツール１６１が収集可能なメタデータが存在する場合この製品について監視付きリリースが要求された場合、その製品を待ち行列Ｂ３（監視付きリリース・プロセス８０６）上に置くあるいはコンテンツ処理ツール１５５のステップＣ４（暗号化プロセス８１１）からのすべての情報が存在する場合、この製品を先行待ち行列（メタデータＳＣ作成プロセス８０７）上に置くあるいは暗号化キーを必要とすることを示すフラグをその製品に付け、この製品を待ち行列Ａ２（製品待受けアクション／情報プロセス８０１）上に置くあるいはメタデータ・プロバイダが強制監視付きリリースを要求した場合、その製品を待ち行列Ｂ３（監視付きリリース・プロセス８０６）上に置くあるいは何も実行しない（その製品を待ち行列Ｂ２（手動メタデータ入力プロセス８０４）上に保持する）
Ｂ３：ステップＢ３（監視付きリリース・プロセス８０６）中にこのオペレータがステップＢ２（手動メタデータ入力プロセス８０４）にその製品を返送する場合、その製品を待ち行列Ｂ２上に置くあるいはこのオペレータがその製品をリリースした場合コンテンツ処理ツール１５５のステップＣ４（暗号化プロセス８１１）からのすべての情報が存在する場合、この製品を先行待ち行列（メタデータＳＣ作成プロセス８０７）上に置くあるいは暗号化キーを必要とすることを示すフラグをその製品に付け、この製品を待ち行列Ａ２（製品待受けアクション／情報プロセス８０１）上に置くあるいはその製品は待ち行列Ｂ２（監視付きリリース・プロセス８０６）上に存続する
先行：先行ステップ（メタデータＳＣ作成プロセス８０７）後にメタデータがパックされたことを示すフラグをその製品に付けるすべての（製品／品質レベル）タプルがパックされた場合コンテンツ・プロバイダ１０１の構成がＳＣの品質保証を指定する場合、この製品を待ち行列Ａ３（最終品質保証プロセス８１３）上に置くあるいはこの製品を待ち行列Ａ４（コンテンツ分散プロセス８１４）上に置くあるいはコンテンツ１１３のＳＣを必要とすることを示すフラグをその製品に付け、この製品を待ち行列Ａ２（製品待受けアクション／情報プロセス８０１）上に置く
Ｃ１：ステップＣ１（ウォータマーク・プロセス８０８）後にステップＣ２（前処理圧縮プロセス８０９）に必要なメタデータが存在する場合、各（製品／品質レベル）タプルごとに項目を作成し、それを待ち行列Ｃ２上に置くあるいは前処理／圧縮用のメタデータを必要とすることを示すフラグをその製品に付け、この製品を待ち

行列Ａ２（製品待受けアクション／情報プロセス８０１）上に置く
Ｃ２：ステップＣ２（前処理圧縮プロセス８０９）後にコンテンツ・プロバイダ１０１の構成がコンテンツ品質管理プロセス８１０を指定する場合、この（製品／品質レベル）タプルを待ち行列Ｃ３（コンテンツ品質管理プロセス８１０）上に置くあるいはこの（製品／品質レベル）タプルを待ち行列Ｃ４（暗号化プロセス８１１）上に置く
Ｃ３：ステップＣ３（コンテンツ品質管理プロセス８１０）後に、この（製品／品質レベル）タプルを待ち行列Ｃ４（暗号化プロセス８１１）上に置く
Ｃ４：ステップＣ４（暗号化プロセス８１１）後に必要な情報（すなわち、そのプロセスによって生成され、コンテンツ１１３を暗号化するために使用する対称キー６２３）をメタデータ同化入力ツール１６１に供給するコンテンツＳＣ６３０に必要なすべてのメタデータが存在する場合、この（製品／品質レベル）タプルを待ち行列Ｃ５（コンテンツＳＣ作成プロセス８１２）上に置くあるいはコンテンツＳＣ６３０のパッキングのためにメタデータを必要とすることを示すフラグをその製品に付け、この（製品／品質レベル）タプルをＡ２（製品待受けアクション／情報プロセス８０１）上に置く
Ｃ５：ステップＣ５（コンテンツＳＣ作成プロセス８１２）後にこの品質レベルのコンテンツ１１３がパックされたことを示すフラグをその品質レベルに付けるすべての（製品／品質レベル）タプルがパックされた場合メタデータがパックされたことを示すフラグがその製品に付けられた場合コンテンツ・プロバイダ１０１の構成がＳＣの品質保証を指定する場合、この製品を待ち行列Ａ３（最終品質保証プロセス８１３）上に置くあるいはこの製品を待ち行列Ａ４（コンテンツ分散プロセス８１４）上に置くあるいはメタデータＳＣ６２０を必要とすることを示すフラグをその製品に付け、この製品を待ち行列Ａ２（製品待受けアクション／情報プロセス８０１）上に置くあるいは（すべての（製品／品質レベル）タプルがパックされていない）何も実行しない（他の（製品／品質レベル）タプルがアクションを起動する
【０２１５】Ｃ．メタデータ同化入力ツール
メタデータはコンテンツ１１３を記述するデータからなり、たとえば音楽では録音のタイトル、アーチスト、著者／作曲家、プロデューサ、録音の長さからなる。以下の説明はコンテンツ１１３が音楽である場合に基づくものであるが、当業者であれば、その他のコンテンツ・タイプ、たとえば、ビデオ、プログラム、マルチメディア、映画、およびそれと同等のものが本発明の真の範囲および意味に含まれることに留意されたい。
【０２１６】このサブシステムは、製品の販売のプロモーションを支援するためにコンテンツ・プロバイダ１０１が電子ディジタル・コンテンツ・ストア１０３に提供するデータ（たとえば、音楽の場合、このアーチストによるサンプル・クリップ、このアーチストの経歴、この録音が収録されたアルバムのリスト、このアーチストまたは製品あるいはその両方に関連するジャンル）、購入した製品とともにコンテンツ・プロバイダ１０１がエンドユーザに提供するデータ（たとえば、アーチスト、プロデューサ、アルバム・カバー、トラック長）、コンテンツ・プロバイダ１０１がエンドユーザに提供したいと希望する各種購入オプション（使用条件５１７）をひとまとめにものである。このデータはメタデータＳＣ６２０にパッケージ化され、電子ディジタル・コンテンツ・ストア１０３が使用可能なものになる。これを実施するため、以下のツールが用意されている。
・　自動メタデータ収集ツール
・　手動メタデータ入力ツール
・　使用条件ツール
・　監視付きリリース・ツール
【０２１７】これらのツールは、コンテンツ・プロバイダ１０１がワーク・フロー・マネージャ１５４に関して前述したプロセスを実施できるようにするものである。ここに記載するツールは、好ましい実施形態ではJavaに基づくツールキットであるが、Ｃ／Ｃ＋＋、アセンブラ、およびそれと同等のものなど、その他のプログラミング言語も使用することができる。
【０２１８】１．自動メタデータ収集ツール
自動メタデータ収集ツールは、前述の自動メタデータ収集プロセス８０３を実施する能力をユーザに提供する。自動メタデータ収集ツールは、コンテンツ・プロバイダ１０１のデータベース１６０にアクセスし、オペレータの支援なしにできるだけ多くのデータを取り出すために使用する。このプロセスを自動化するために、構成方法が使用可能である。コンテンツ・プロバイダ１０１は、このコンテンツ・プロバイダ１０１がエンドユーザに提供したいと希望するデータのタイプ（たとえば、作曲家、プロデューサ、伴奏楽器奏者、トラック長）およびコンテンツ・プロバイダ１０１が電子ディジタル・コンテンツ・ストア１０３に提供するプロモーション・データのタイプ（たとえば、音楽の例の場合、このアーチストによるサンプル・クリップ、このアーチストの経歴、この録音が収録されたアルバムのリスト、このアーチストに関連するジャンル）を識別するためにデフォルト・メタデータ・テンプレートを調整することができる。デフォルト・メタデータ・テンプレートとしては、エンドユーザ装置１０９が必要とするデータ・フィールド、任意選択でエンドユーザ装置１０９に提供可能なデータ・フィールド、電子ディジタル・コンテンツ・ストア１０３を目標とし、アーチスト、アルバム、またはシングル、あるいはそれらの組合せをプロモーションする複数データ・フィールドからなるサンプル・セットを含む。
【０２１９】コンテンツ・プロバイダ１０１のデータベ

ース１６０からテンプレート・データ・フィールドを抽出するために、自動メタデータ収集ツールは、データのタイプ（たとえば、作曲家、プロデューサ、アーチストの経歴）をデータを検出可能なデータベース内の位置にマッピングするテーブルを使用する。各コンテンツ・プロバイダ１０１は、それぞれの環境用にマッピング・テーブルを指定するのを支援する。

【０２２０】自動メタデータ収集ツールは、コンテンツ・プロバイダ１０１のメタデータ・テンプレートとマッピング・テーブルを使用して、コンテンツ・プロバイダ１０１のデータベース１６０から入手可能なものであればどのようなデータでも収集する。各製品の状況は自動メタデータ収集プロセス８０３の結果によって更新される。何らかの必須データが欠落している製品は手動メタデータ入力プロセス８０４のために待ち行列化され、そうでない場合、その製品はメタデータＳＣ６２０にパックするために使用可能である。

【０２２１】２．手動メタデータ入力ツール

手動メタデータ入力ツールは、前述の手動メタデータ入力プロセス８０４を実施する能力をユーザに提供する。手動メタデータ入力ツールは、適切に許可されたオペレータが欠落データを提供できるようにするものである。欠落データが使用不能であるとオペレータが判断した場合、そのオペレータは製品にコメントを付加し、監視付きリリースを要求することができる。コンテンツ・プロバイダ１０１は、品質保証のために、その製品に対して監視付きリリースを行うことを要求することができる。すべての必須データが存在し、しかも監視付きリリースがまだ要求されていない場合、その製品はメタデータＳＣ６２０にパックするために使用可能である。

【０２２２】３．使用条件ツール

使用条件ツールは、前述の使用条件プロセス８０５を実施する能力をユーザに提供する。電子送達を使用して販売または賃貸借（限定使用）のためにコンテンツ１１３を提供するプロセスは一連のビジネス判断を必要とする。コンテンツ・プロバイダ１０１は、コンテンツ１１３を使用可能にする圧縮レベルを決定する。次に、コンテンツ１１３の各圧縮コード化バージョンごとに、１つまたは複数の使用条件を指定する。各使用条件は、コンテンツ１１３の使用に関してエンドユーザの権利とエンドユーザに対する制限を定義する。

【０２２３】コンテンツ処理ツール１５５の一部として、１組の使用条件（エンドユーザの権利および制限）が製品に付加される。

【０２２４】１つの使用条件は以下のものを定義する。

１．この使用条件が適用されるコンテンツ１１３の圧縮コード化バージョン

２．この使用条件が適用されるユーザのタイプ（たとえば、企業、個人消費者）

３．この使用条件がコンテンツ１１３の購入を可能にするか賃貸借を可能にするか

賃貸借トランザクションの場合：

・　賃貸借の期間を限定するために使用する測定単位（たとえば、日数、再生回数）

・　それ以降コンテンツ１１３がもはや再生されなくなる上記の単位数購入トランザクションの場合：

・　エンドユーザが作成を許される再生可能コピーの数

・　コピーを作成可能な媒体の種類（たとえば、ＣＤレコーダブル（ＣＤ－Ｒ）、ミニディスク、パーソナル・コンピュータ）

４．購入／賃貸借トランザクションを行える期間（すなわち、エンドユーザは、使用可能開始日後であってしかも使用可能最終日前に限り、この使用条件の条件下で購入／賃貸借を行うことができる）

５．エンドユーザがこの購入（または賃貸借）のトランザクションを行うことができる国

６．この使用条件下での購入／賃貸借トランザクションの価格

７．ウォータマーク・パラメータ

８．クリアリング・ハウス１０５の通知を必要とするイベントのタイプ

【０２２５】使用条件のセットの例

コンテンツ・プロバイダ１０１は、１９９７年の第４四半期中に人気のある子供向け歌手による子供向け歌曲の再リリースを北米市場が受け入れるかどうかをテストすることを決定する場合がある。このテストでは、この歌曲を３８４Ｋｂｐｓと５６Ｋｂｐｓという２通りの圧縮コード化バージョンで提供する。３８４Ｋｂｐｓバージョンは購入（およびミニディスク上に１回コピー可能）または賃貸借（２週間）可能であり、５６Ｋｂｐｓバージョンは購入のみ（コピー作成は不可）可能である。ウォータマーク命令はいかなる購入／賃貸着荷ついても同じであり、コンテンツ・プロバイダ１０１は作成したすべてのコピーをクリアリング・ハウス１０５がカウントすることを希望する。これは、使用条件を以下のように作成することになるだろう。

【０２２６】

【表１０】

	使用条件１	使用条件２	使用条件３
圧縮コード化バージョン	384Kbps	384Kbs	56Kbps
ユーザのタイプ	個人消費者	個人消費者	個人消費者
トランザクションのタイプ	購入	賃貸借	購入
使用可能日	1997年10月1日～1997年12月31日	1997年10月1日～1997年12月31日	1997年10月1日～1997年12月31日
国	米国およびカナダ	米国およびカナダ	米国およびカナダ
ウォータマーク	標準	標準	標準
通知イベント	コピー処置	なし	なし
コピー回数	1	0	0
媒体	ミニディスク	適用不可	適用不可
賃貸借期間	適用不可	14日間	適用不可
価格	価格１	価格２	価格３

【０２２７】４．メタデータＳＣ６２０の各パーツメタデータＳＣ６２０に含めるためにメタデータ同化入力ツール１６１が収集するデータの種類の一部を以下に示す。関数および宛先別にＳＣの各パーツにデータをグループ化しようと試みたものである。

【０２２８】

製品ＩＤ　[ソース：コンテンツ・プロバイダ]　[宛先：全員；]

ライセンス許諾者レコード会社　[宛先：ＥＭＳ；エンドユーザ；]

ライセンス保持者レコード会社　[宛先：ＥＭＳ；エンドユーザ；]

このオブジェクト（二次ライセンス保持者レコード会社）のソース（発行者）　[宛先：全員；]

オブジェクトのタイプ（すなわち、単一オブジェクトまたは複数オブジェクトのアレイ）

オブジェクトＩＤ　[宛先：全員；]

国際標準記録コード（ＩＳＲＣ）

国際標準音楽番号（ＩＳＭＮ）

使用条件（ソース：コンテンツ・プロバイダ；宛先：ＥＭＳ、エンドユーザ、クリアリング・ハウス１０５）

購入済み使用条件（ソース：ＥＭＳ；宛先：エンドユーザ、クリアリング・ハウス１０５）

オブジェクト（録音）の使用のための使用条件のセット（消費者の制限および権利）

使用条件のアレイ内の個々の項目

この使用条件が適用されるコンテンツ１１３の圧縮コード化バージョン

この使用条件がコンテンツ１１３の購入を可能にするか賃貸借を可能にするか

賃貸借トランザクションの場合：

賃貸借の期間を限定するために使用する測定単位（たとえば、日数、再生回数）

それ以降コンテンツ１１３がもはや再生されなくなる上記の単位数

購入トランザクションの場合：

エンドユーザが作成を許される再生可能コピーの数

コピーを作成可能な媒体の種類（たとえば、ＣＤレコーダブル（ＣＤ－Ｒ）、ミニディスク、パーソナル・コンピュータ）

購入／賃貸借トランザクションを行える期間（すなわち、エンドユーザは、使用可能開始日後であってしかも使用可能最終日前に限り、この使用条件の条件下で購入／賃貸借を行うことができる）

エンドユーザがこの購入（または賃貸借）のトランザクションを行うことができる国を指し示すポインタ

この使用条件下での購入／賃貸借トランザクションの価格

暗号化ウォータマーク命令およびパラメータを指し示すポインタ

クリアリング・ハウス１０５の通知を必要とするイベントのタイプを指し示すポインタ
購入データ（暗号化；任意選択情報；ソース：ＥＭＳ；宛先：エンドユーザ、クリアリング・ハウス１０５）
購入日
購入価格
請求先の名前と住所
消費者の名前と住所
消費者の国（最良推測）
メタデータ１（ソース：コンテンツ・プロバイダ；宛先：ＥＭＳ、エンドユーザ）
アレイ｛
著作権情報
作曲の場合
録音の場合
歌曲のタイトル
主要アーチスト
｝
ポインタ｛
アートワーク（たとえば、アルバム・カバー）
アートワークのフォーマット（たとえば、ＧＩＦ、ＪＰＥＧ）
｝
任意選択情報：
追加情報のアレイ｛
作曲家
発行者
プロデューサ
伴奏楽器奏者
録音日
リリース日
歌詞
トラック名（説明）／トラック長
この録音が収録されたアルバムのリスト
ジャンル
｝
メタデータ２（ソース：コンテンツ・プロバイダ；宛先：ＥＭＳ）
複数構造のアレイ、それぞれは同じ録音の異なる品質レベルを表す｛
録音；
録音の品質レベル；
（おそらく圧縮された）録音のサイズ（バイト単位）
｝
メタデータ３（ソース：コンテンツ・プロバイダ；宛先：ＥＭＳ、エンドユーザ）
任意選択情報：
プロモーション素材：
アーチスト・プロモーション素材を指し示すポインタ｛
アーチストのウェブ・サイトへのＵＲＬ；
アーチストの背景説明；
アーチスト関連インタビュー（インタビューのフォーマット（たとえば、テキスト、オーディオ、ビデオ）付き）；

評論（評論のフォーマット（たとえば、テキスト、オーディオ、ビデオ）付き）；
サンプル・クリップ（およびそのフォーマットと圧縮レベル）；
最近および今後のコンサート／出演／イベント　－　それぞれの日付および場所；
｝
アルバム・プロモーション素材を指し示すポインタ｛
サンプル・クリップ（およびそのフォーマットと圧縮レベル）；
プロデューサまたは作曲家、映画／演劇／配役、アルバム作成などの背景説明；
非アーチスト関連インタビュー（インタビューのフォーマット（たとえば、テキスト、オーディオ、ビデオ）付き）；
評論（評論のフォーマット（たとえば、テキスト、オーディオ、ビデオ）付き）；
ジャンル；
｝
シングル・プロモーション：
サンプル・クリップ（およびそのフォーマットと圧縮レベル）
プロデューサまたは作曲家、映画／演劇／配役、シングル作成などの背景説明；
評論（評論のフォーマット（たとえば、テキスト、オーディオ、ビデオ）付き）

【０２２９】５．監視付きリリース・ツール
監視付きリリース・ツールは、前述の監視付きリリース・プロセス８０６を実施する能力をユーザに提供する。監視付きリリース権限を有するものとしてコンテンツ・プロバイダ１０１が指定した個人は、監視付きリリースを待っている製品（すなわち、監視付きリリース・プロセス８０６の待ち行列上にある製品）を呼び出し、そのコンテンツ１１３とその付随コメントを検査し、以下のいずれかを行うことができる。そのコンテンツ１１３を承認し、メタデータＳＣ６２０にパックするためにその製品をリリースするか、必要な訂正を加え、メタデータＳＣ６２０にパックするためにその製品をリリースするか、実行すべき訂正アクションを指定するコメントを追加し、手動メタデータ入力プロセス７０４に製品を再提示する。
【０２３０】他の実施形態には、ＳＣの作成後、もう１つの任意選択の品質保証ステップが存在し、そこではＳＣのコンテンツ１１３をオープンし、完璧さおよび正確さについて検査することができ、その時点で、小売経路へのその製品のリリースについて最終承認を与えるかまたは拒否することができる。
【０２３１】Ｄ．コンテンツ処理ツール
コンテンツ処理ツール１５５は、実際には、ディジタル・コンテンツ・ファイルを処理し、コンテンツのウォータマーク付きコード化暗号化コピーを作成するために使用するソフトウェア・ツールの集合である。これらのツールは、業界標準のディジタル・コンテンツ処理ツールを利用し、ウォータマーク、コード化、および暗号化の諸技術が進化するにつれてその技術を差込み交換できるようにする。選択した業界ツールがコマンド行システム呼出しインタフェースによりロードされ、それにパラメータを渡すことができるか、またはＤＬＬインタフェースにより関数を呼び出すことができるツールキットを提供する場合、そのコンテンツ処理はある程度まで自動化することができる。各ツールへのフロントエンド・アプリケーションは、次の使用可能なジョブについてコンテンツ処理ツール１５５内の適切な待ち行列に照会し、必須ファイルおよびパラメータを取り出し、業界標準のコンテンツ処理ツールをロードして必須関数を実行する。そのタスクが完了すると、そのツールが終了状況を報告しない場合、待ち行列への手動更新が必要になる場合もある。
【０２３２】コンテンツ処理ツール１５５の汎用バージョンについて説明するが、カストマイズも可能である。コンテンツ処理ツール１５５は、Java、Ｃ／Ｃ＋＋、それと同等のソフトウェアで作成することができる。また、コンテンツ処理ツール１５５は、ディスケット、ＣＤを含むコンピュータ可読手段あるいはウェブ・サイトにより送達することができる。
【０２３３】１．ウォータマーク・ツール
ウォータマーク・ツールは、前述のウォータマーク・プロセス８０８を実施する能力をユーザに提供する。このツールは、オーディオ・ウォータマーク技術を使用して歌曲ファイルにコンテンツ１１３のオーナの著作権情報を適用する。書き出される実際の情報は、コンテンツ・プロバイダ１０１と、選択した特定のウォータマーク技

術によって決定される。この情報は、それがこの情報をウォータマーク機能に適切に渡すことができるように、フロントエンド・ウォータマーク・ツールにとって使用可能なものである。これは、たとえば、歌曲のオーディオ・ファイルを処理できるようにする前にこの情報を取得したことを保証するために、メタデータ同化入力ツール１６１に同期要件を課すものである。この歌曲は、ウォータマーク情報が入手されるまで、オーディオ処理に使用可能な状態にならない。

【０２３４】ウォータマークは、作成した歌曲のすべてのコード化に共通なものなので、オーディオ処理の第１のステップとして適用される。ウォータマークがコード化技術以降も存続可能な限り、ウォータマーク・プロセスは１曲につき１回だけ行えばよい。

【０２３５】様々なウォータマーク技術が知られており、市販されている。しかし、フロントエンド・ウォータマーク・ツールは、様々な業界用ウォータマーク・ツールをサポートすることができる。

【０２３６】２．前処理圧縮ツール

前処理圧縮ツールは、前述の前処理圧縮プロセス８０９を実施する能力をユーザに提供する。オーディオ・コード化は２つのプロセスを必要とする。コード化は、基本的に、音楽コンテンツの例の場合はＰＣＭオーディオ・ストリームに対して損失圧縮アルゴリズムを適用することである。通常、エンコーダは、必要なオーディオ品質のレベルに基づいて様々な再生ビット・ストリーム・レートを生成するように調整することができる。品質が高くなると結果的にファイル・サイズが大きくなり、高品質コンテンツ１１３の場合、ファイル・サイズは非常に大きいものになる可能性があるので、高品質コンテンツ１１３のダウンロード時間は長々しく、時には標準の２８８００ｂｐｓモデム上で非常に高いものになる可能性がある。

【０２３７】したがって、コンテンツ・プロバイダ１０１は、１回のダウンロードのために何時間も待ちたくない性急で低帯域幅の顧客と、高品質コンテンツ１１３のみを購入するかより高速の接続を有するオーディオファンまたは広帯域幅の顧客の両方をなだめるために、ダウンロード用に様々なディジタル・コンテンツ品質を提示することを選ぶことができる。

【０２３８】圧縮アルゴリズムは、コンテンツ１１３を低ビット伝送速度で複製するためのそれぞれの技術が異なる。この技術は、アルゴリズムごと（すなわち、ＭＰＥＧ、ＡＣ３、ＡＴＲＡＣ）および圧縮レベルごとに異なる。より高レベルの圧縮を達成するために、通常、データは、圧縮アルゴリズムに送達される前により低いサンプリング速度で再サンプリングされる。忠実度の損失が低く、より効率の良い圧縮を可能にするために、またはいくつかの周波数範囲の激烈なドロップアウトを防止するために、ディジタル・コンテンツは、所与の周波数の等化レベルに応じた調整または録音の強弱の変化に応じた調整を必要とする場合もある。コンテンツの前処理要件は、圧縮アルゴリズムおよび必要な圧縮のレベルに直接関連する。場合によっては、コンテンツ１１３のスタイル（たとえば、音楽ジャンル）は前処理要件を決定するためのベースとして正常に使用することができる。というのは、同じジャンルの複数の歌曲は通常、同様の強弱の変化を有するからである。一部の圧縮ツールでは、このような前処理機能はコード化プロセスの一部である。他のツールでは、圧縮の前に所望の前処理が実行される。

【０２３９】販売用のダウンロード可能なオーディオ・ファイルに加え、各歌曲は、低ビット伝送速度（ＬＢＲ）コード化クリップも有し、その歌曲をＬＢＲストリーミング・プロトコルによってサンプリングできるようにする。このＬＢＲコード化はコンテンツ処理ツール１５５の責任でもある。このクリップは、個別のＰＣＭファイルとしてまたはオフセットと長さのパラメータとしてコンテンツ・プロバイダ１０１によって提供される。

【０２４０】ウォータマークの場合のように、コード化ツールがＤＬＬまたはコマンド行システム呼出しインタフェースによりロード可能であり、前処理および圧縮のためのすべての必須パラメータが渡されることが期待される。フロントエンド・コード化ツールは、たとえば、コンテンツが音楽であり、オーディオ前処理を実行する前にその歌曲のジャンルがコンテンツ・プロバイダのデータベース１６０から取得されると判定された場合、メタデータ同化入力ツール１６１との同期要件を有する可能性がある。これは、選択したコード化ツールと、その歌曲のジャンルがどのように不確定であるかによって決まる。コンテンツ・プロバイダ１０１が１曲あたりのコード化品質レベルの選択を変更する場合、この情報もコード化ステップの前に提供され、メタデータ同化入力ツール１６１によって生成されるメタデータと一致する。

【０２４１】今日、様々な高品質コード化アルゴリズムおよびツールが知られている。しかし、フロントエンド・コード化ツールは、様々な業界用コード化ツールをサポートすることができる。

【０２４２】次に図１５に移行すると、本発明により図１１の自動メタデータ収集ツール用の一実施形態の流れ図が示されている。このプロセスは、コンテンツ・プロバイダ１０１が検査する媒体から識別子を読み取ることから始まる。コンテンツの一例はオーディオＣＤの実施形態である。オーディオＣＤの実施形態では、ユニバーサル価格コード（ＵＰＣ）、国際標準記録コード（ＩＳＲＣ）、国際標準音楽番号（ＩＳＭＮ）というコードが使用可能である可能性がある。ステップ１２０１で、コンテンツ用の適切なプレーヤ、たとえば、オーディオＣＤ用のオーディオＣＤプレーヤ、ＤＶＤ映画用のＤＶＤプレーヤ、ＤＡＴ録音用のＤＡＴレコーダ、およびそれ

と同等のものでこの識別子を読み取る。次に、ステップ１２０２で、この識別子を使用してコンテンツ・プロバイダ１０１用のデータベース１６０に索引を付ける。ステップ１２０３では、図１１に記載したようにワーク・フロー・マネージャ・プロセスが必要とする情報の一部または全部をデータベース１６０およびその他の関連ソースから取り出す。この情報は、コンテンツ１１３と、それに関連するメタデータを含むことができる。ステップ１２０４では、取り出した追加情報を使用して、電子コンテンツ１１３を作成するためにワーク・フロー・マネージャ１５４を開始する。ただし、自動メタデータ収集ツールが電子配布のために一連のコンテンツ１１３を作成できるように、複数のオーディオＣＤなど、複数媒体の選択肢を待ち行列化することができることに留意されたい。たとえば、すべてのコンテンツ１１３は、一連のＣＤまたはコンテンツ・プロバイダ１０１が検査した１つまたは複数のＣＤから選択したトラックから作成することができるだろう。

【０２４３】代替実施形態では、コンテンツ・プロバイダのデータベース１６０から自動的に前処理パラメータを取り出すことができる。次に図１６を参照すると、本発明により図１１の前処理圧縮ツールの前処理圧縮パラメータを自動的に設定するための方法の流れ図が示されている。この実施形態のコンテンツ１１３は音楽である。ステップ１３０１では、コンテンツ処理ツール１５５でコード化すべき音楽（コンテンツ１１３）を選択する。ステップ１３０２では、選択した音楽のジャンルを決定する。これは、手動で入力するかまたは図１５に記載したプロセスから取り出した追加データなど、他の使用可能なメタデータを使用することにより入力することができる。次にステップ１３０３では、選択したオーディオ圧縮レベルおよびオーディオ圧縮アルゴリズムを検査する。次にステップ１３０４では、ジャンルによって、ルックアップを行い、前処理圧縮プロセス８０９でどの圧縮パラメータを使用すべきかについての圧縮設定および圧縮アルゴリズムを選択する。

【０２４４】３．コンテンツ品質管理ツール

コンテンツ品質管理ツールは、前述のコンテンツ品質管理プロセス８１０を実施する能力をユーザに提供する。これは、任意選択のコンテンツ処理ツールであり、品質管理専門家がコード化しウォータマークを付けたコンテンツ・ファイルを検討し、品質判断に基づいてそのコンテンツ・ファイルを承認または拒否するための機会を提供する。その専門家は、その品質が妥当なものになるまで手動前処理調整を行ってそのコンテンツを再コード化することができ、あるいは再処理用のフラグをその歌曲に付け、問題を記述する注を付加することができる。

【０２４５】このプロセス・ステップは、コンテンツ処理ワーク・フローの任意選択ステップまたは必須ステップとしてコンテンツ・プロバイダ１０１が構成することができる。このコンテンツ用のすべてのＳＣ（たとえば、１枚のＣＤ上の複数歌曲用の各ＳＣ）のパッケージ化後に、最終品質保証プロセス８１３の追加かつ任意選択のステップが用意されており、その時点でコンテンツ・コード化の品質をテストすることができるが、暗号化およびパッケージ化の前に早めに問題を把握すると、より効率の良いコンテンツ処理が可能になる。したがって、すべての処理の最終完了まで待つこととは対照的に、このステップでコンテンツ品質を保証することは非常に望ましいことである。

【０２４６】４．暗号化ツール

暗号化ツールは、前述の暗号化プロセス８１１を実施する能力をユーザに提供する。コンテンツ暗号化はコンテンツ処理ツール１５５の最終ステップである。コード化ツールによって作成されたコンテンツの各バージョンをここで暗号化する。暗号化ツールはＳＣパッカの機能の１つである。ＳＣパッカを呼び出して歌曲を暗号化し、使用した生成暗号化キーを返す。その後、このキーは、メタデータＳＣ６２０の作成時に使用するためにＳＣパッカに渡される。

【０２４７】Ｅ．コンテンツＳＣ作成ツール

すべてのメタデータが収集されると、コンテンツＳＣ作成ツールはそれぞれの所期の用途に基づいてそのメタデータをカテゴリ別にグループ化する。これらのメタデータ・グループは、メタデータＳＣ６２０用のメタデータ・パーツとしてＳＣパッカ・ツールに渡されるファイル内に作成される。各パーツ（ファイル）は固有の処理要件を有する。関連歌曲が処理され暗号化され、ターゲット宛先（コンテンツ・ホスト・サイト１１１のＵＲＬ）が決定されると、コンテンツ１１３用のコンテンツＳＣ６３０はいつでも作成できる状態になる。処理が完了し、前述のすべての要件を満たしたコンテンツ１１３は、ワーク・フロー・マネージャ１５４のパッカ待ち行列にパックするために待ち行列化される。

【０２４８】次にコンテンツＳＣ作成ツールは、メタデータ同化入力ツール１６１の先行ステップによって作成されたすべての必須ファイルを取り出し、ＳＣパッカ機能を呼び出してメタデータＳＣ６２０およびコンテンツＳＣ６３０を作成する。このプロセスは、各歌曲ごとに単一のメタデータＳＣ６２０と複数のコンテンツＳＣ６３０を作成する。たとえば、コンテンツが音楽である場合、歌曲全体の様々な品質レベルに関するオーディオ処理中に作成した各オーディオ・ファイルを別々のコンテンツＳＣ６３０にパックする。サンプル・クリップ用に作成したオーディオ・ファイルは、メタデータＳＣ６２０に含めるメタデータ・ファイルとして渡される。

【０２４９】Ｆ．最終品質保証ツール

最終品質保証ツールは、前述の最終品質保証プロセス８１３を実施する能力をユーザに提供する。１つのコンテンツ・ファイルについてすべてのＳＣが構築されると、

そのコンテンツは最終品質保証チェックに使用可能な状態になる。品質保証は、コンテンツ１１３の作成プロセスの様々な段階で実行することができる。コンテンツ・プロバイダ１０１は、その後の過度の手直しを防止するために各主要ステップが完了するたびに品質保証を実行することを選択することができ、あるいはすべてのオーディオ作成プロセスが完了するまで待ち、すべてについて一度に品質保証を実行することを選択することもできる。後者を選択した場合、ＳＣの作成が完了すると、この時点で品質保証が実行される。このツールにより、その歌曲用の各ＳＣをオープンして検査し、オーディオ再生することができる。

【０２５０】いずれかの問題が検出されると、わずかなテキスト変更でも、ＳＣの内部セキュリティ機構によりＳＣを再構築しなければならない。不必要な再処理時間を回避するため、暫定品質保証ステップを使用してメタデータの正確さを保証することと、この歌曲に関連するＳＣ間の適切な相互参照を妥当性検査するためにこの特定の品質保証ステップを予約することが非常に推奨される。問題が検出された場合、保証者は、歌曲に付加すべき問題記述を入力し、それを再処理のために適切な処理待ち行列に再待ち行列化することができる。歌曲のすべての関連コンポーネントの状況を示すように、ワーク・フロー・マネージャ１５４内で適切に状況を更新する。いかなる問題も検出されない場合、コンテンツ１１３にはリリース可能を示すマークまたはフラグが付けられる。

【０２５１】Ｇ．コンテンツ分散ツール

コンテンツ分散ツールは、前述のコンテンツ分散プロセス８１４を実施する能力をユーザに提供する。リリースのためにコンテンツ１１３が承認されると、コンテンツ１１３用のＳＣはコンテンツ分散プロセスの待ち行列内に置かれる。コンテンツ分散ツールは待ち行列を監視し、コンテンツ・プロバイダ１０１によって提供された構成設定に基づいてＳＣファイルの即時転送または１群のＳＣファイルのバッチ転送を実行する。また、コンテンツ・プロバイダ１０１は任意選択で、リリースのために手動でフラグが付けられるまですべてのＳＣをこの待ち行列内に自動的に保持するようにコンテンツ分散ツールを構成することもできる。これにより、コンテンツ・プロバイダ１０１は、スケジューリングしたリリース日に先だってコンテンツを作成し、たとえば、新しい歌曲、映画、またはゲームなど、それをリリースしたいと希望するようになるまでそれを保持することができる。また、ＳＣは定義済みリリース日に基づいてコンテンツ１１３へのアクセスを制御することもできるので、コンテンツ・プロバイダ１０１が実際にＳＣの送達を止めるための要件は一切存在しないが、この手動リリース・オプションは依然としてこの目的に使用するかまたはこれらの大型ファイルを転送するために必要なネットワーク帯域幅を管理するために使用することができる。

【０２５２】リリースのためにフラグが付けられると、コンテンツ１１３用のコンテンツＳＣ６３０はＦＴＰにより指定のコンテンツ・ホスト・サイト１１１に転送される。メタデータＳＣ６２０はＦＴＰによりコンテンツ・プロモーション・ウェブ・サイト１５６に転送される。この場合、ＳＣは、処理し、コンテンツ・プロモーション・ウェブ・サイト１５６に統合できるようになるまで、コンテンツ１１３の新しいディレクトリにステージングされる。

【０２５３】図２１は、本発明により図１１の自動メタデータ収集ツール用の追加情報を自動的に検索するための代替実施形態の流れ図である。このプロセスは、上記の図１１に記載したものと同様のものである。しかし、監視付きリリース８０６およびコンテンツ品質管理８０９の品質チェックは、品質管理１７０４という１つの品質チェックに結合されている。メタデータＳＣ作成８０７およびコンテンツＳＣ作成８１２の前に品質チェックを実行する。ＳＣ作成の前に品質チェックを実行すると、コンテンツ１１３および関連メタデータＳＣ６２０をアンパックするステップが除去される。そのうえ、この実施形態では、製品待受けアクション／情報８０１の待ち行列が除去されている。ジョブは、どのアクションが要求されているかに応じて、特定のプロセス待ち行列上に置かれる。たとえば、そのジョブが手動メタデータ、すなわち、追加メタデータの入力を必要とする場合、そのジョブは手動メタデータ入力待ち行列上に置かれる。また、自動メタデータ収集８０３は、メタデータ同化入力ツール１６１およびコンテンツ処理ツール１５５より前に前もって行われるように、新コンテンツ要求と併合されている。最後に、使用条件８０４が自動メタデータ収集８０３と手動メタデータ入力８０３時の両方で入力されることを指摘しておくことは重要なことである。その後、使用条件の多くは自動メタデータ収集８０３のステップ中に自動的に記入することができる。

【０２５４】Ｈ．コンテンツ・プロモーション・ウェブ・サイト

コンテンツ・プロバイダ１０１がディジタル・ダウンロードにより販売用に使用可能にするものに関する情報を最も効果的に分散するために、また、それがこのコンテンツ１１３をその顧客へのダウンロード用に使用可能な状態にすることができるように電子ディジタル・コンテンツ・ストア１０３に必要なファイルを取得するために、各コンテンツ・プロバイダ１０１は、この情報を収容する安全なウェブ・サイトを持っていなければならない。これは、この情報を必要とするその小売業者およびその他のものに対してプロモーション・コンテンツを使用可能な状態にするために、現在、一部のコンテンツ・プロバイダ１０１が使用する方法と同様のものである。このタイプのサービスがすでに存在する場合、電子ディ

ジタル・コンテンツ・ストア１０３がダウンロードにより販売用に使用可能なコンテンツのリストを見に行けるような追加のセクションをそのウェブ・サイトに追加することができる。

【０２５５】コンテンツ・プロバイダ１０１は、このサイトの設計およびレイアウトを完全に制御しているか、またはセキュア・ディジタル・コンテンツ電子配布システム１００用のツールキットの一部として提供されるターンキー・ウェブ・サーバ・ソリューションの使用を選択することができる。このサービス用のそれぞれの設計を実施するために、コンテンツ・プロバイダ１０１は、それぞれのサイトにアクセスする電子ディジタル・コンテンツ・サーバ１０３用のメタデータＳＣ６２０へのリンクを用意するだけでよい。これは、セキュア・ディジタル・コンテンツ電子配布システム１００用のツールキットを使用して実施される。この選択プロセスおよびどの情報が示されるかは、コンテンツ・プロバイダ１０１の自由裁量である。

【０２５６】コンテンツ分散ツールからＦＴＰにより新しいコンテンツ・ディレクトリ内に受け取ったメタデータＳＣ６２０は、コンテンツ・プロモーション・ウェブ・サイト１５６によって処理される。これらのコンテナは、コンテナから情報を表示または抽出するためにＳＣプリビュー・ツールによってオープンすることができる。次に、この情報を使用して、ＨＴＭＬウェブ・ページを更新するかまたはこのサービスによって維持されるサーチ可能データベースに情報を追加することができる。ＳＣプリビュー・ツールは、実際には、メタデータＳＣ６２０をオープンして処理するために電子ディジタル・コンテンツ・ストア１０３が使用するコンテンツ収集ツールのサブセットである。詳細についてはコンテンツ収集ツールの項を参照されたい。次に、メタデータＳＣ６２０ファイルは、コンテンツ・プロモーション・ウェブ・サイト１５６によって維持される永続ディレクトリに移動しなければならない。

【０２５７】メタデータＳＣ６２０がコンテンツ・プロモーション・ウェブ・サイト１５６に統合されると、その可用性が公表される。コンテンツ・プロバイダ１０１は、それぞれの新しいメタデータＳＣ６２０がそのサイトに追加されるたびにすべての加入電子ディジタル・コンテンツ・ストア１０３に通知を送ることができ、あるいはその日（または期間）に追加されたすべてのメタデータＳＣ６２０に関する単一通知を毎日（またはいずれかの定義済み周期で）実行することができる。この通知は、追加されるメタデータＳＣ６２０を参照するパラメータを含む定義済みＣＧＩストリングを送ることにより、電子ディジタル・コンテンツ・ストア１０３ウェブ・サーバとの標準のＨＴＴＰ交換により実行される。このメッセージは、後述する電子ディジタル・コンテンツ・ストア１０３の通知インタフェース・モジュールによって処理される。

【０２５８】Ｉ．コンテンツ・ホスト

エンターテイメント業界は、毎年、ＣＤ、映画、ゲームなど、何千ものコンテンツ・タイトルを制作し、現在入手可能な何万ものコンテンツ・タイトルをさらに増大させている。セキュア・ディジタル・コンテンツ電子配布システム１００は、現在、店頭で入手可能なすべてのコンテンツ・タイトルをサポートするように設計されている。

【０２５９】最終的にセキュア・ディジタル・コンテンツ電子配布システム１００が毎日、顧客に対してダウンロード可能なコンテンツ・タイトルの数は数千または数万である。タイトルが多数の場合、これは大量の帯域幅を必要とする。このようなコンピュータ・ディスク空間および帯域幅の必要性により、複数のコンテンツ・ホスト・サイト１１１による分散スケーラブル実施が要求される。また、このシステムは、世界中の顧客をサポートする。このため、全世界に渡る顧客への送達を促進するために海外サイトが必要になる。

【０２６０】セキュア・ディジタル・コンテンツ電子配布システム１００上のコンテンツ・ホストは、コンテンツ・プロバイダ１０１がそれ自身のコンテンツ１１３のホストとなるかあるいは１つの共通設備または１組の設備を共用することができるように設計されている。

【０２６１】セキュア・ディジタル・コンテンツ電子配布システム１００上のコンテンツ・ホストは、セキュア・ディジタル・コンテンツ電子配布システム１００によって提供されるコンテンツ１１３のすべてをひとまとめにして含む複数のコンテンツ・ホスト・サイト１１１と、コンテンツ・プロバイダ１０１によって提供される現行ホット・ヒットを含む複数の２次コンテンツ・サイト（図示せず）からなる。コンテンツ・ホスト・サイト１１１の数は、このシステムを使用するエンドユーザの数に応じて変化する。２次コンテンツ・サイトは限られた数の歌曲のホストとなるが、このシステム上で使用する帯域幅の多くの部分を表すことになる。２次サイトは、１次サイト上のボリュームが最大容量の点まで増大するとオンラインになる。２次サイトはネットワーク・アクセス・ポイント（ＮＡＰ）付近に位置することができ、これはダウンロード時間を加速するのに役に立つ。また、２次サイトは、ダウンロード時間を加速するために世界中の様々な地域に配置することもできる。

【０２６２】コンテンツ・プロバイダ１０１がそれ自体のシステム内のすべてのコンテンツ１１３のホストとなることを選択した場合、追加の２次コンテンツ・サイトの有無にかかわらず、単一のコンテンツ・ホスト・サイト１１１として動作することができる。このため、それ自体のスケーラブル分散システムを構築することができる。他の実施形態では、電子ディジタル・コンテンツ・ストア１０３も所与のコンテンツ１１３用のコンテンツ

・ホスト・サイト１１１として動作することができる。この実施形態では、電子ディジタル・コンテンツ・ストア１０３とコンテンツ・プロバイダ１０１との間の特別な財政上の合意が必要である。

【０２６３】１．コンテンツ・ホスト・サイト

コンテンツ１１３は、本明細書のコンテンツ・プロバイダの項で説明したコンテンツ分散ツールによるＦＴＰまたはＨＴＴＰによるかあるいはテープ、ＣＤ－ＲＯＭ、フラッシュ、その他のコンピュータ可読媒体上でのコンテンツ送達などのオフライン手段により、コンテンツ・ホスト・サイト１１１に追加される。コンテンツ・プロバイダ１０１によって作成されたメタデータＳＣ６２０は、このコンテンツ１１３用のコンテンツＳＣ６３０を突き止めるＵＲＬを示すフィールドを含む。このＵＲＬはコンテンツ・ホスト・サイト１１１に対応する。電子ディジタル・コンテンツ・ストア１０３は、コンテンツ・プロバイダ１０１によって許される場合、オファーＳＣ６４１内でこのＵＲＬを指定変更することができる。エンドユーザ装置１０９は、コンテンツＳＣ６３０をダウンロードしたいと希望する場合、このコンテンツ・ホスト・サイト１１１に連絡する。

【０２６４】エンドユーザ装置１０９は、コンテンツ・ホスト・サイト１１１にライセンスＳＣ６６０を送ることにより、コンテンツＳＣ６３０を求める要求を開始する。これは、クリアリング・ハウス１０５によって返されるのと同じライセンスＳＣ６６０である。ライセンスＳＣ６６０のディジタル・シグニチャを検証すると、それが有効なライセンスＳＣ６６０であるかどうかを判定することができる。それが有効なライセンスＳＣ６６０である場合、ダウンロードが開始されるかまたはダウンロード要求を他のコンテンツ・ホスト・サイト１１１にリダイレクトすることができる。

【０２６５】２．セキュア・ディジタル・コンテンツ電子配布システム１００によって提供されるコンテンツ・ホスト・サイト１１１

セキュア・ディジタル・コンテンツ電子配布システム１００の場合、どのサイトを使用してコンテンツ１１３をダウンロードするかという判断は、コンテンツＳＣ６３０を求める初期要求を受け取った１次コンテンツ・サイトによって行われる。このサイトでは以下の情報を使用してこの判断を行う。

・　要求したコンテンツ１１３のホストとなる２次コンテンツ・サイトが存在するか。（セキュア・ディジタル・コンテンツ電子配布システム１００によって提供されるコンテンツ１１３の大部分は１次サイトにのみ位置する。）

・　エンドユーザ装置１０９は地理的にどこに位置するか。（この情報は、その要求がエンドユーザ装置１０９で開始されたときにはエンドユーザ装置１０９から入手することができ、これはオーダＳＣ６５０に入れてクリアリング・ハウス１０５に渡される。）

・　適切な２次サイトが機能しているか。（場合によっては、２次サイトがオフラインになっている可能性がある。）

・　２次サイトの負荷は何か。（２次サイトが活動資めにあっている場合、あまり混んでいない他のサイトを選択することもできる。）

【０２６６】エンドユーザ装置１０９にコンテンツＳＣ６３０を伝送する前に、エンドユーザの要求で分析および検証が行われる。コンテンツ１１３をダウンロードするために使用したすべてのライセンスＳＣ　ＩＤのデータベースを保持する。このデータベースをチェックして、エンドユーザ装置１０９が購入したコンテンツ１１３の各ピースごとに１つの要求のみ行うことを保証することができる。このため、悪意のあるユーザは、コンテンツ・ホスト・サイト１１１の速度低下を期待してコンテンツ・ホスト・サイト１１１に繰返しアクセスすることができなくなり、コンテンツＳＣ６３０の無許可ダウンロードが防止される。

【０２６７】２次コンテンツ・サイトへのコンテンツ１１３のプロモーションとデモーションは、コンテンツ１１３の個々のピースに対する顧客の需要に基づいて定期的に行われる。

【０２６８】コンテンツ・ホスト・ルータ

コンテンツ・ホスト・ルータ（図示せず）は、コンテンツ・ホスト・サイト１１１内に存在し、コンテンツ１１３をダウンロードしようと待っているエンドユーザからのすべての要求を受け取る。このルータは、エンドユーザの要求に対する妥当性検査を実行し、そのエンドユーザが本当にコンテンツ１１３を購入したことを保証する。どのコンテンツ１１３がそこに存在するかとその現行状況を含む、２次コンテンツ・サイトの状況に関するデータベースが維持される。この現行状況としては、そのサイト上での活動量と、サイトがメンテナンスのために停止しているかどうかを含む。

【０２６９】コンテンツ・ホスト・ルータへの唯一のインタフェースはライセンスＳＣ６６０であり、このＳＣはコンテンツ１１３をダウンロードする必要があるときにエンドユーザ装置１０９によって送られる。ライセンスＳＣ６６０は、そのユーザがコンテンツ１１３をダウンロードできることを示す情報を含む。

【０２７０】２次コンテンツ・サイト

２次コンテンツ・サイト（図示せず）は、セキュア・ディジタル・コンテンツ電子配布システム１００の人気のあるコンテンツ１１３のホストとなる。これらのサイトは、地理的には世界中に分散し、ダウンロード時間を改善するためにネットワーク・アクセス・ポイント（ＮＡＰ）付近に位置する。これらのサイトは、１次コンテンツ・ホスト・サイト１１１での需要に応じて最大容量付近までシステムに追加される。

【０２７１】IX. 電子ディジタル・コンテンツ・ストアA. 概要ー複数電子ディジタル・コンテンツ・ストア１０３のサポート
電子ディジタル・コンテンツ・ストア１０３は本質的に小売業者である。これは、顧客に配布すべきコンテンツ１１３をマーケティングするエンティティである。コンテンツ１１３の配布の場合、これは、ディジタル・コンテンツ小売ウェブ・サイト、ディジタル・コンテンツ小売ストア、または顧客への電子コンテンツ１１３のマーケティングにかかわりたいと希望する企業を含むことになるだろう。これらの企業は電子コンテンツ１１３のみの販売をマーケティングすることができるかまたは現在、販売のために提供しているその他の商品に電子商品の販売を追加することを選択することができる。ダウンロード可能な電子商品を電子ディジタル・コンテンツ・ストア１０３のサービス・オファリングに取り入れることは、セキュア・ディジタル・コンテンツ電子配布システム１００の一部として電子ディジタル・コンテンツ・ストア１０３用に開発された１組のツールにより実施される。
【０２７２】このようなツールは、以下の動作のために電子ディジタル・コンテンツ・ストア１０３が使用する。
・　コンテンツ・プロバイダ１０１によってパッケージ化されたメタデータＳＣ６２０を取得する。
・　これらのＳＣからコンテンツ１１３を抽出して、そのサービス・オファリングを構築するための入力として使用する。
・　販売のために提供するダウンロード可能なコンテンツ１１３を記述するオファーＳＣ６４１を作成する。
・　トランザクションＳＣ６４０を作成してエンドユーザ装置１０９に送ることにより、販売の肯定応答およびダウンロードの開始を処理する。
・　ダウンロード可能なコンテンツ１１３の販売と各ダウンロードの状況を示すトランザクション・ログを管理する。
・　状況通知およびトランザクション認証要求を処理する。
・　会計調停を実行する。
【０２７３】これらのツールは、電子ディジタル・コンテンツ・ストア１０３がダウンロード可能な電子コンテンツ１１３の販売をそのサービスに統合したいと希望する際に柔軟性を見込むように設計されている。これは必須ではないが、購入したダウンロード可能なコンテンツ１１３に関するすべての金融決済がクリアリング・ハウス１０５によって処理されることを要求するように、これらのツールを使用することができる。また、これらのツールは、電子ディジタル・コンテンツ・ストア１０３がその顧客に完全に対応し、プロモーションおよび特殊オファーの提供を含む、金融トランザクション自体を処理できるようにする。これらのツールは、電子ディジタル・コンテンツ・ストア１０３がダウンロード可能なコンテンツ１１３の販売をその既存サービスに迅速に統合できるようにする。そのうえ、電子ディジタル・コンテンツ・ストア１０３は、ダウンロード可能なコンテンツ１１３のホストとなる必要がなく、その分散を管理する必要もない。この機能は、コンテンツ・プロバイダ１０１が選択したコンテンツ・ホスト・サイト１１１によって実行される。
【０２７４】電子ディジタル・コンテンツ・ストア１０３用のツールは、好ましい実施形態ではJavaで実現されているが、Ｃ／Ｃ＋＋、アセンブラ、それと同等のものなど、他のプログラミング言語も使用することができる。ただし、電子ディジタル・コンテンツ・ストア１０３に関して後述するツールは様々なハードウェアおよびソフトウェア・プラットフォームで動作可能であることに留意されたい。完全なシステムとしてまたはその構成コンポーネントの一部としての電子ディジタル・コンテンツ・ストア１０３は、ウェブなどの電子配布またはフロッピー・ディスケット、ＣＤ－ＲＯＭ、取外し可能ハード・ディスク・ドライブを含みかつこれに限定されないコンピュータ可読媒体に入れてアプリケーション・プログラムとして配布することができる。
【０２７５】他の実施形態では、電子ディジタル・コンテンツ・ストア１０３のコンポーネントはプログラマのソフトウェア・ツールキットの一部である。このツールキットにより、後述する電子ディジタル・コンテンツ・ストア１０３の汎用コンポーネントおよびツールの各種コンポーネントへの事前定義インタフェースが可能になる。このような事前定義インタフェースは、ＡＰＩまたはアプリケーション・プログラミング・インタフェースの形式になっている。このようなＡＰＩを使用する開発者は、高レベル・アプリケーション・プログラムから各種コンポーネントの機能性のいずれかを実現することができる。このようなコンポーネントにＡＰＩを提供することにより、プログラマは、これらのコンポーネントのいずれかの機能およびリソースを再作成する必要なしに、カストマイズした電子ディジタル・コンテンツ・ストア１０３を迅速に開発することができる。
【０２７６】電子ディジタル・コンテンツ・ストア１０３は、ウェブ・ベースのサービス・オファリングに限定されない。提供されるツールは、このコンテンツ１１３をエンドユーザに送達するために使用する伝送インフラストラクチャまたは送達モードにかかわらず、ダウンロード可能な電子コンテンツ１１３を販売したいと希望するすべての電子ディジタル・コンテンツ・ストア１０３が使用する。衛星およびケーブル・インフラストラクチャにより提供される同報通信サービスも同じツールを使用して、電子コンテンツ１１３の販売を取得し、パッケージ化し、追跡する。販売のための電子商品の提示およ

びこれらのオファーがエンドユーザに送達される方法は、同報通信ベースのサービス・オファリングとポイントツーポイント対話ウェブ・サービス・タイプのオファリングとの間の主な変形である。

【０２７７】Ｂ．ポイントツーポイント電子ディジタル・コンテンツ配布サービス

ポイントツーポイントは、主に、電子ディジタル・コンテンツ・ストア１０３とエンドユーザ装置１０９との間の１対１の対話サービスを意味する。これは、通常、電話またはケーブル・モデム接続によって提供されるインターネット・ウェブ・ベースのサービスを表す。インターネット以外のネットワークも、ウェブ・サーバ／クライアント・ブラウザ・モデルに適合する限り、このモデルでサポートされる。図１２は、電子ディジタル・コンテンツ・ストア１０３の主要ツール、コンポーネント、プロセスを示すブロック図である。

【０２７８】１．統合要件

セキュア・ディジタル・コンテンツ電子配布システム１００は、新しいオンライン・ビジネスを創出するだけでなく、既存のビジネスがダウンロード可能な電子コンテンツ１１３の販売をその現行在庫に統合するための方法も提供する。電子ディジタル・コンテンツ・ストア１０３に提供されるツール一式は、この統合努力を簡略化する。コンテンツ収集ツール１７１とＳＣパッカ・ツール１５３は、電子ディジタル・コンテンツ・ストア１０３が販売のために使用可能な状態で持っているものに関する情報を参加コンテンツ・プロバイダ１０１から収集し、このようなダウンロード可能なオブジェクトをそのプロバイダ自体の在庫内の項目として参照するために必要なファイルを作成するための方法を提供する。このプロセスは、バッチ駆動され、大部分は自動化することができ、新しいコンテンツ１１３をそのサイト内に統合するためにのみ実行される。

【０２７９】セキュア・ディジタル・コンテンツ電子配布システム用のツールは、その現行コンテンツ１１３小売パラダイムに最小限の変更を加えることにより、ウェブ・ベースの電子ディジタル・コンテンツ・ストア１０３の典型的な実施例（すなわち、Columbia Houseオンライン、Music Boulevard、Tower）およびそれと同等なものにダウンロード可能な電子コンテンツ１１３の販売を統合できるように設計されている。いくつかの統合方法が可能であり、好ましい実施形態では、電子ディジタル・コンテンツ・ストア１０３はすべての製品サーチ、プリビュー、選択（ショッピング・カート）、購入をサポートする。各電子ディジタル・コンテンツ・ストア１０３は、その顧客とともに顧客への忠誠を確立し、それ自体の刺激策を提供し、現在行っているようにその製品のマーケティングを続行する。セキュア・ディジタル・コンテンツ電子配布システム１００では、その在庫内のどの製品が電子ダウンロードに使用可能であるかを示し、購入選択を行うときにその顧客が電子ダウンロード・オプションを選択できるようにすることが必要になるだけであろう。他の実施形態では、顧客のショッピング・カートは電子媒体選択（コンテンツ１１３）と物理媒体選択の混合物を含む可能性がある。顧客がチェックし、電子ディジタル・コンテンツ・ストア１０３が金融決済を完了し、購入した物理的商品を処理するためにその発送処理機能をログ記録するかまたは通知した後、電子ディジタル・コンテンツ・ストア１０３の商取引処理機能はトランザクション・プロセッサ・モジュール１７５を呼び出してすべての電子ダウンロードを処理する。これは必須情報を渡すだけであり、その時点からのすべての処理はセキュア・ディジタル・コンテンツ電子配布システム１００用のツールセットによって処理される。他の実施形態では、電子ディジタル・コンテンツ・ストア１０３がダウンロード可能な商品の販売のみを希望するかまたは物理的商品とダウンロード可能な商品の金融決済の分離を希望する場合、金融決済を処理するためにセキュア・ディジタル・コンテンツ電子配布システム１００用のツールを使用する他のトランザクション処理方法も可能である。

【０２８０】諸品のダウンロードを処理するために、電子ディジタル・コンテンツ・ストア１０３には、それがコンテンツ・プロバイダ１０１用のコンテンツ・プロモーション・ウェブ・サイト１５６から取得するダウンロード可能な各製品ごとに製品ＩＤ（図示せず）が与えられる。この製品ＩＤは、ダウンロード可能な製品に対する顧客の購入選択に関連付けられている。製品ＩＤは、ユーザが購入した製品を識別するために電子ディジタル・コンテンツ・ストア１０３がトランザクション・プロセッサ・モジュール１７５に渡すものである。製品を記述するために作成されたＳＣ（オファーＳＣ６４１）は、電子ディジタル・コンテンツ・ストア１０３から分離され、このようなオブジェクトの管理を簡略化し、その存在を電子ディジタル・コンテンツ・ストア１０３にとって透過的なものにしようとして、オファー・データベース１８１内に保持される。

【０２８１】トランザクション・プロセッサ・モジュール１７５およびその他の追加機能は、ウェブ・サーバ側の実行可能機能（すなわち、ＣＧＩおよびＮＳＡＰＩ、ＩＳＡＰＩ呼出し可能機能）または単なるＡＰＩとしてＤＬＬまたはＣオブジェクト・ライブラリに用意される。これらの機能は、クリアリング・ハウス１０５とのエンドユーザ対話および任意選択対話のランタイム処理を取り扱う。これらの機能は、ウェブ・サーバの商取引サービスと対話して、コンテンツ１１３のダウンロード・プロセスを開始するために必要なファイルを作成し、それをエンドユーザ装置１０９にダウンロードする。また、これらは、認証を行い、活動の完了通知を受け入れるための任意選択対話も処理する。

【０２８２】それ自体およびクリアリング・ハウス１０５のトランザクション・ログに基づいて会計を調停するためにクリアリング・ハウス１０５に連絡する際に電子ディジタル・コンテンツ・ストア１０３を支援するように、会計調停ツール１７９も用意されている。

【０２８３】２．コンテンツ収集ツール１７１

コンテンツ収集ツール１７１は、メタデータＳＣ６２０をプリビューしダウンロードするためにコンテンツ・プロモーション・ウェブ・サイト１５６とのインタフェースを担当する。コンテンツ・プロモーション・サイトは標準のウェブ・サイトなので、このサイトをナビゲートするために電子ディジタル・コンテンツ・ストア１０３はウェブ・ブラウザを使用する。ナビゲーション機能は、コンテンツ・プロバイダ１０１のサイト設計に基づいて様々である。一部のサイトは、多くのプロモーション情報画面によって広範囲なサーチ機能を提供する可能性がある。その他のサイトは、そこから選択するためにタイトル、演奏者、新リリースのリストを備えた単純なブラウザ・インタフェースを有する可能性がある。どのサイトも、１つの歌曲またはアルバムのプロモーション情報および記述情報のすべてを含むメタデータＳＣ６２０の選択を含んでいる。

【０２８４】あるいは、電子ストア１０３は、コンテンツ更新に加入し、ＦＴＰにより自動的に更新内容を受け取ることもできる。

【０２８５】メタデータの閲覧

コンテンツ収集ツール１７１は、コンテンツ・プロモーション・ウェブ・サイト１５６でメタデータＳＣ６２０リンクが選択されたときに必ず立ち上がるウェブ・ブラウザ・ヘルパ・アプリケーションである。そのＳＣを選択すると、それが電子ディジタル・コンテンツ・ストア１０３にダウンロードされ、ヘルパ・アプリケーションが立ち上がる。コンテンツ収集ツール１７１はメタデータＳＣ６２０をオープンし、そこに含まれる非暗号化情報を表示する。表示される情報としては、抽出メタデータ１７３を含み、音楽の例の場合、その歌曲に関連するグラフィック・イメージとその歌曲を記述する情報を含み、メタデータＳＣ６２０に含まれていれば、その歌曲のプリビュー・クリップも聞くことができる。コンテンツ１１３が音楽である一例では、コンテンツ・プロバイダ１０１によって提供されていれば、その歌曲またはアルバムに関するプロモーション情報、アルバム・タイトル、アーチストも示される。この情報は、一連のリンク付きＨＴＭＬページとしてブラウザ・ウィンドウに表示される。歌曲や歌詞などの購入可能コンテンツ１１３と、コンテンツ・プロバイダ１０１が保護したいと希望するその他のメタデータは、小売コンテンツ・ウェブ・サイト１８０にとってアクセス不能なものである。

【０２８６】他の実施形態では、コンテンツ・プロバイダ１０１は、所定の手数料で任意選択のプロモーション・コンテンツを提供する。この実施形態では、このようなプロモーション・コンテンツはメタデータＳＣ６２０で暗号化される。このデータをオープンするための金融決済は、指定の手数料が請求される電子ディジタル・コンテンツ・ストア１０３用の口座を備えたクリアリング・ハウス１０５によって処理することができる。

【０２８７】メタデータの抽出

プリビュー機能に加え、このツールは、メタデータ抽出とオファーＳＣ６４１の作成という２つの追加機能を提供する。メタデータ抽出オプションを選択すると、電子ディジタル・コンテンツ・ストア１０３は、そのメタデータが記憶されるパスおよびファイル名の入力を要求される。グラフィックおよびオーディオ・プリビュー・クリップなどの２進メタデータは別々のファイルとして記憶される。テキスト・メタデータは、小売コンテンツ・ウェブ・サイト１８０がそのデータベース内にインポート可能なＡＳＣＩＩ区切りテキスト・ファイルに記憶される。そのＡＳＣＩＩ区切りファイルのレイアウトを記述するテーブルも個別のＴＯＣファイルに作成される。その他の各国語サポート（ＮＬＳ）がサポートするフォーマットへの抽出を可能にするために、追加のオプションも使用可能である。

【０２８８】抽出データとして提供される重要な情報の１つは製品ＩＤである。この製品ＩＤは、ユーザが購入したコンテンツ１１３をトランザクション・プロセッサ・モジュール１７５（詳細についてはトランザクション処理の項を参照）に対して識別するために電子ディジタル・コンテンツ・ストア１０３用の商取引処理機能が必要とするものである。トランザクション・プロセッサ・モジュール１７５はこの製品ＩＤを使用して、エンドユーザ装置１０９への今後のダウンロードのために適切なオファーＳＣ６４１をオファー・データベース１８１から正しく取り出す。電子ディジタル・コンテンツ・ストア１０３は、それがダウンロード可能なコンテンツ１１３をそのサイト上で提示する方法を完全に制御する。セキュア・ディジタル・コンテンツ電子配布システム１００用のツールとのインタフェースを適切に取るためには、この製品ＩＤと提供中のコンテンツ１１３との相互参照を保持することだけが必要である。この情報をここで提供すると、電子ディジタル・コンテンツ・ストア１０３は、オファーＳＣ６４１の作成プロセスと並行してこの製品またはコンテンツ１１３をその在庫および販売ページ（データベース）に統合することができる。というのは、どちらのプロセスも、製品を参照するために同じ製品ＩＤを使用するからである。これについては以下に詳述する。

【０２８９】オファーＳＣ作成パッカ１５３

電子ディジタル・コンテンツ・ストア１０３は、販売用のダウンロード可能なコンテンツ１１３を記述するオファーＳＣ６４１を作成する必要がある。オファーＳＣ６

４１内に入る情報のほとんどはメタデータＳＣ６２０から導出される。コンテンツ収集ツール１７１は以下の操作によりオファーＳＣ６４１を作成する。

・　メタデータＳＣ６２０内でオファーＳＣテンプレートによって定義されたオファーＳＣ６４１に含める必要がないパーツをメタデータＳＣ６２０から除去する。

・　電子ディジタル・コンテンツ・ストア１０３のためにこのツール内の構成オプションで指定されたデフォルトによって定義された追加の必須パーツを追加する。

・　メタデータＳＣ６２０内でオファーＳＣテンプレートによって定義された追加の必須入力または選択を要求する。

・　この情報をＳＣフォーマットにパックするためにＳＣパッカ１５３を呼び出す。

【０２９０】エンドユーザ装置１０９上にプレーヤ・アプリケーション１９５（以下に詳述する）によって表示されるメタデータはメタデータＳＣ６２０に保持される。そのウェブ・サービス・データベースへの入力として電子ディジタル・コンテンツ・ストア１０３のみが使用したその他のプロモーション・メタデータはメタデータＳＣ６２０から除去される。ウォータマーク命令、暗号化対称キー６２３、そのオブジェクトの許可用途を定義する使用条件５１７など、コンテンツ・プロバイダ１０１によって提供される権利管理情報も保持される。

【０２９１】この余計なものを省いたメタデータＳＣ６２０はオファーＳＣ６４１に含まれる。電子ディジタル・コンテンツ・ストア１０３は、ストア使用条件５１９というそれ自体の使用条件または購入オプションもオファーＳＣ６４１に付加する。これは、１組のデフォルトにより自動的にまたは対話式に実施することができる。対話式に処理するように構成した場合、電子ディジタル・コンテンツ・ストア１０３は、コンテンツ・プロバイダ１０１によって定義された１組の許可オブジェクト使用条件５１７により指示される。次に、そのストアは自分の顧客に対して提供したいオプションを選択する。これらは新しい使用条件またはストア使用条件５１９になる。自動的に処理するために、電子ディジタル・コンテンツ・ストア１０３は、すべてのコンテンツ１１３について提供すべき１組のデフォルト購入オプションを構成する。これらのデフォルト・オプションは、コンテンツ・プロバイダ１０１が定義した許可使用条件５１７と照らし合わせて自動的にチェックされ、矛盾がなければオファーＳＣ６４１内に設定される。

【０２９２】オファーＳＣ６４１が作成されると、それはオファー・データベース１８１に記憶され、メタデータＳＣ６２０で事前割当てされた製品ＩＤで索引が付けられる。この製品ＩＤは、オファー・データベース１８１とのインタフェースを取り、パッケージ化およびエンドユーザへの伝送のためにオファーＳＣ６４１を取り出す際に、顧客が購入するダウンロード可能なコンテンツ１１３を識別するために後で電子ディジタル・コンテンツ・ストア１０３が使用する。詳細についてはトランザクション・プロセッサ・モジュール１７５の項を参照されたい。

【０２９３】他の実施形態では、電子ディジタル・コンテンツ・ストア１０３は自分のサイトでコンテンツＳＣ６４１のホストとなる。この実施形態では、コンテンツ・ホスト・サイト１１１のＵＲＬを電子ディジタル・コンテンツ・ストア１０３のＵＲＬで置き換えるなど、オファーＳＣ６４１に変更を加える必要がある。

【０２９４】３．トランザクション処理モジュール１７５

電子ディジタル・コンテンツ・ストア１０３はクリアリング・ハウス１０５に請求を振り向ける。あるいは、電子ディジタル・コンテンツ・ストア１０３は、クリアリング・ハウス１０５から直接、金融決済を要求することができる。ダウンロード可能なコンテンツ１１３を求めるエンドユーザ購入要求を処理するために、２通りの基本モードが存在する。電子ディジタル・コンテンツ・ストア１０３がその購入の金融決済を処理することを希望せず、その商品の販売を左右する特殊プロモーションまたは刺激策を一切持っておらず、しかも購入要求をバッチ処理するためにショッピング・カート・メタフォーを使用しない場合、そのコンテンツ１１３ダウンロード・ページ上にオファーＳＣ６４１ファイルに直接至るリンクを設けることを選ぶことができる。このようなオファーＳＣ６４１は、メタデータに含まれる小売価格設定情報とともに構築しておく必要があるだろう。また、オファーＳＣ６４１には、販売の条件とともに購入オプションを提示する特殊ＨＴＭＬオファー・ページも含まれる。このページは、オファーＳＣ６４１が構築されたときに作成したテンプレートから構築される。エンドユーザがオファーＳＣ６４１への直接リンクをクリックすると、オファーＳＣ６４１はブラウザにダウンロードされ、エンドユーザ装置１０９はヘルパ・アプリケーションを立ち上げて、コンテナをオープンし、オファーＳＣ６４１に含まれるオファー・ページを提示する。このページは、クレジット・カード情報および購入オプション選択を含む顧客情報を収集するための書式を含む。この書式は、金融決済および処理のためにクリアリング・ハウス１０５に直接提示される。任意選択で、この書式は、エンドユーザのクレジット情報または業界標準のローカル・トランザクション・ハンドラを使用するために必要なフィールドを含むことができる。

【０２９５】次に、電子ディジタル・コンテンツ・ストア１０３が請求を処理する実施形態について説明する。より典型的な購入要求処理モードでは、電子ディジタル・コンテンツ・ストア１０３が金融決済を処理し、ダウンロード認証をエンドユーザに提示することができる。この方法では、電子ディジタル・コンテンツ・ストア１

０３はダウンロード可能なコンテンツ１１３の販売とそのサイトで販売するために提供されたその他の商品とを統合することができ、各ダウンロード要求ごとの個別請求ではなく（ショッピング・カート・メタフォーによる）顧客への１回の統合請求のみにより購入要求のバッチ処理が可能になり、電子ディジタル・コンテンツ・ストア１０３がその顧客購入パターンを直接追跡し、特殊プロモーションおよびクラブ・オプションを提供することができる。この実施形態では、ダウンロード可能なコンテンツ１１３のオファーがそのショッピング・ページに含まれ、それは、エンドユーザが選択したときにショッピング・カートに追加され、電子ディジタル・コンテンツ・ストア１０３の現行ショッピング・モデルで行われるように処理され金融決済される。金融決済が完了すると、電子ディジタル・コンテンツ・ストアの商取引処理プロセスはトランザクション・プロセッサ・モジュール１７５を呼び出して、トランザクションを完了する。

【０２９６】トランザクション・プロセッサ・モジュール１７５

トランザクション・プロセッサ・モジュール１７５の役割は、購入したコンテンツ１１３のダウンロードを開始し処理するためにエンドユーザ装置１０９が必要とする情報をまとめることである。この情報は、購入提示に対する応答としてウェブ・サーバによってエンドユーザ装置１０９に返送されるトランザクションＳＣ６４０にパッケージ化される。トランザクション・プロセッサ・モジュール１７５は、電子ディジタル・コンテンツ・ストア１０３の商取引処理プロセスからの３つの情報、すなわち、購入したコンテンツ１１３用の製品ＩＤ、トランザクション・データ６４２、購入決済を確認するＨＴＭＬページまたはＣＧＩ　ＵＲＬを必要とする。

【０２９７】製品ＩＤは、販売したばかりのコンテンツ１１３に関連するメタデータＳＣ６２０に入れて電子ディジタル・コンテンツ・ストア１０３に提供される値である。この製品ＩＤは、オファー・データベース１８１から関連のオファーＳＣ６４１を取り出すために使用する。

【０２９８】トランザクション・データ６４２は、クリアリング・ハウス１０５の処理を電子ディジタル・コンテンツ・ストア１０３によって実行される金融決済トランザクションと相関させ、エンドユーザ装置１０９にダウンロードされるコンテンツ１１３のウォータマークに含めるユーザ・アイデンティティ情報を提供するために後で使用する電子ディジタル・コンテンツ・ストア１０３のトランザクション処理機能によって提供される情報の構造体である。クリアリング・ハウス１０５は、有効なオーダＳＣ６５０を受け取ると、販売されたコンテンツ１１３、どの電子ディジタル・コンテンツ・ストア１０３がそれを販売したか、エンドユーザの名前およびトランザクションＩＤ５３５を含む関連トランザクション・データ６４２を示すトランザクションをログ記録する。トランザクションＩＤ５３５は、金融決済トランザクションへの参照を示す。この情報は、コンテンツ・プロバイダ１０１（またはそのエージェント）から受け取った請求明細によってその口座を調停する際に使用するために、後でクリアリング・ハウス１０５によって電子ディジタル・コンテンツ・ストア１０３に返される。クリアリング・ハウス・トランザクション・ログ１７８は、自分のどのコンテンツ１１３が販売されたかを判定するためにコンテンツ・プロバイダ１０１が使用することができ、そのプロバイダはそれが負っている使用料に関し各電子ディジタル・コンテンツ・ストア１０３への請求書を作成することができる。あるいは、請求以外のその他の電子手段を使用して、コンテンツ・プロバイダ１０１と電子ディジタル・コンテンツ・ストア１０３との間で会計を決済することもできる。

【０２９９】トランザクションＳＣ６４０で提供される情報とトランザクションＳＣ６４０のセキュリティおよび完全性により、購入トランザクションが有効であるという十分な信憑性がクリアリング・ハウス１０５にもたらされ、したがって、クリアリング・ハウス１０５によりこの販売をログ記録する前にそれ以上の妥当性検査は不要になる。しかし、電子ディジタル・コンテンツ・ストア１０３は、その口座に請求される前に認証を要求することができる（クリアリング・ハウス１０５でログ記録されたトランザクションは、この電子ディジタル・コンテンツ・ストア１０３がこのコンテンツ１１３の販売に関する金銭を集金したことをコンテンツ・プロバイダ１０１に示す）。認証／通知を求めるこの要求はトランザクション・データ６４２内のフラグによって示される。このシナリオでは、クリアリング・ハウス１０５は電子ディジタル・コンテンツ・ストア１０３に連絡し、自分の口座への請求および暗号化キー６２３のリリースの前に電子ディジタル・コンテンツ・ストア１０３から認可を受ける。トランザクションＩＤ５３５は、この認証要求の一部としてクリアリング・ハウス１０５から電子ディジタル・コンテンツ・ストア１０３に渡され、電子ディジタル・コンテンツ・ストア１０３がこの要求をエンドユーザによって実行された先行トランザクションに関連付けることができるようにする。このトランザクションＩＤ５３５は、電子ディジタル・コンテンツ・ストア１０３が使用したいと希望する任意の固有値にすることができ、単にそのストアのためだけのものである。

【０３００】トランザクション・データ６４２は顧客名も含む。この名前は、購入を行うときにユーザが記入した購入書式のユーザ名フィールドから得るか、または電子ディジタル・コンテンツ・ストア１０３での何らかのユーザ登録プロセス中に事前にログ記録された情報から得るか、あるいはこのトランザクションで使用したカードに関連するクレジット・カード情報から得た公式名に

することができる。この名前は、後でライセンス・ウォータマーク５２７に含まれる。

【０３０１】トランザクション・データ６４２は、エンドユーザが購入したストア使用条件５１９も含む。この情報は、ライセンス・ウォータマーク５２７に含まれ、コピー再生制御においてエンドユーザ装置１０９が使用する。

【０３０２】トランザクション・プロセッサ・モジュール１７５が必要とする最終パラメータは、購入決済を確認するＨＴＭＬページまたはＣＧＩ　ＵＲＬである。その目的は、電子ディジタル・コンテンツ・ストア１０３が金融決済の肯定応答およびその応答に含めたいと希望するその他の情報によってエンドユーザに応答できるようにすることである。このＨＴＭＬページまたはＣＧＩ　ＵＲＬは、トランザクションＳＣ６４０に含まれ、トランザクションＳＣ６４０を受け取って処理したときにエンドユーザ装置１０９のブラウザ・ウィンドウに表示される。

【０３０３】トランザクションＳＣ６４０は、購入提示を処理した後に電子ディジタル・コンテンツ・ストア１０３からエンドユーザに送られるＨＴＴＰ応答である。直接ＨＴＴＰ応答としてＳＣを送ると、エンドユーザ装置１０９へのＳＣプロセッサ・ヘルパ・アプリケーションの自動ロードが強制的に行われ、その結果、それ以上のエンドユーザ開始アクションに依存せずにトランザクションの自動完了が可能になる。このプロセスについては、以下のエンドユーザ装置１０９およびプレーヤ・アプリケーション１９５の項で詳述する。

【０３０４】必須パラメータを指定してトランザクション・プロセッサ・モジュール１７５が呼び出されると、このモジュールは、トランザクション・データ６４２、トランザクション肯定応答ＨＴＭＬページ、ＳＣのその他の必須セキュリティ機能への参照ＵＲＬを含むトランザクションＳＣ６４０を構築し、この購入に関連するオファーＳＣ６４１を取り出して埋め込む。また、これは、通知インタフェース・モジュール１７６および会計調停ツール１７９が後で使用するためにこのトランザクションに関する情報をログ記録する。

【０３０５】４．通知インタフェース・モジュール１７６

通知インタフェース・モジュール１７６は、ウェブ・サーバ側の実行可能ルーチン（ＣＧＩまたはＮＳＡＰＩ、ＩＳＡＰＩ、またはこれと同等のものによって呼出し可能な機能）である。これは、クリアリング・ハウス１０５、エンドユーザ装置１０９、コンテンツ・ホスト・サイト１１１、コンテンツ・プロバイダ１０１からの任意選択の要求および通知を処理する。電子ディジタル・コンテンツ・ストア１０３が任意選択で通知を要求できるイベントは以下の通りである。

・　エンドユーザ装置１０９が暗号化キー６３２を要求し、クリアリング・ハウス１０５が指定のコンテンツ１１３のために暗号化キー６２３をリリースするというクリアリング・ハウス１０５からの通知。この通知は任意選択で、暗号化キー６２３をエンドユーザ装置１０９に送る前に電子ディジタル・コンテンツ・ストア１０３からの認証を必要とするように構成することができる。

・　コンテンツＳＣ６３０がエンドユーザ装置１０９に送られたというコンテンツ・ホスト・サイト１１１からの通知。

・　コンテンツＳＣ６３０およびライセンスＳＣ６６０が受け取られ、コンテンツ１１３を処理するために正常に使用されたかまたは壊れていることが分かったというエンドユーザ装置１０９からの通知。

・　新しいコンテンツ１１３がコンテンツ・プロモーション・ウェブ・サイト１５６内に置かれたというコンテンツ・プロバイダ１０１からの通知。

【０３０６】これらの通知のいずれも、セキュア・ディジタル・コンテンツ電子配布システム１００のフローの必須ステップではないが、その販売の完了を満たしたときにそのレコードを閉じる機会を電子ディジタル・コンテンツ・ストア１０３に与えるオプションとして用意されている。また、これは、トランザクションの最終決済以降にどの機能が発生したかまたは販売を完了しようと試みている最中にどのエラーが発生したかを電子ディジタル・コンテンツ・ストア１０３に知らせることにより、顧客サービス要求を処理するために必要になると思われる情報も提供する。あるいは、この状況の多くは、必要に応じて顧客サービス・インタフェース１８４によりクリアリング・ハウス１０５から得ることができる。

【０３０７】コンテンツ・プロモーション・ウェブ・サイト１５６で入手可能な新しいコンテンツ１１３の通知頻度はコンテンツ・プロバイダ１０１によって決定される。新しいメタデータＳＣ６２０が追加されるたびにまたは毎日その日に追加されたすべての新しいメタデータＳＣ６２０により、通知を行うことができる。

【０３０８】このような通知のいずれでも、結果的にトランザクション・ログ１７８への入力が行われる。電子ディジタル・コンテンツ・ストア１０３は、このような通知に対してそれ自体の処理を実行したいと希望する場合、ＣＧＩ呼出しをインターセプトし、固有の機能を実行し、任意選択で通知インタフェース・モジュール１７６にその要求を渡すことができる。

【０３０９】５．会計調停ツール１７９

この会計調停ツール１７９は、トランザクション・ログ１７８とクリアリング・ハウス１０５のログを比較するようクリアリング・ハウス１０５に連絡する。これは、セキュア・ディジタル・コンテンツ電子配布システム１００のための会計処理を快適に行えるように電子ディジタル・コンテンツ・ストアを支援するために使用可能な任意選択のプロセスである。

【０３１０】他の実施形態では、コンテンツ・プロバイダ１０１およびクリアリング・ハウス１０５への自動定期支払のために電子資金振替を行えるようにこのツールを更新することができる。また、これは、トランザクション・ログ１７８と照らし合わせて請求内容を調停した後でクリアリング・ハウス１０５から電子請求書を受け取り次第、支払を自動的に処理するように設計することもできる。

【０３１１】Ｃ．同報通信電子ディジタル・コンテンツ配布サービス

同報通信とは、主として、オンデマンド視聴をカストマイズするためにエンドユーザ装置１０９と電子ディジタル・コンテンツ・ストア１０３との間で個人的対話が一切行われない１対多数の伝送方法を意味する。これは通常、すべてのエンドユーザ装置１０９が同じストリームを受け取るようにコンテンツ１１３が事前プログラミングされているディジタル衛星またはケーブル・インフラストラクチャにより提供される。

【０３１２】サイト設計における多大な共通性により、インターネット接続によるウェブ配布インタフェースならびに同報通信サービスによるより高帯域の衛星またはケーブル配布インタフェースの両方を提供できるように構成されたディジタル・コンテンツ・サービスを電子ディジタル・コンテンツ・ストア１０３が提供するようなハイブリッド・モデルも定義することができる。ＩＲＤバック・チャネル・シリアル・インタフェースがウェブに接続され、ＩＲＤがウェブ・ナビゲーションをサポートすれば、エンドユーザはバック・チャネル・インターネット・インタフェースによる通常のやり方でディジタル・コンテンツ・サービスをナビゲートし、購入するためのコンテンツ１１３をプリビューし選択することができるだろう。ユーザは、いずれもインターネット接続により、高品質のダウンロード可能なコンテンツ１１３を選択し、このような選択を購入し、必須ライセンスＳＣ６６０を受け取ることができ、その後、より高帯域の同報通信インタフェースによりコンテンツ１１３（コンテンツＳＣ６３０）の送達を要求することができる。ウェブ・サービスは、同報通信スケジュールに基づいてどのコンテンツ１１３がこのようにダウンロード用に使用可能になるかを示すことができ、あるいは購入したコンテンツ１１３に完全に基づいて同報通信ストリームを構築できるだろう。この方法により、ウェブ・ベースのディジタル・コンテンツ・サービスは同報通信施設と契約を結び、限られた数の特定のコンテンツ１１３（たとえば、歌曲またはＣＤ）をこのようにして毎日使用可能にし、カタログ全体をウェブ・インタフェースによるより低品質のダウンロード用に使用可能にする適切な機器を装備したユーザに高品質コンテンツ１１３を送達することができるだろう。

【０３１３】エンドユーザ装置１０９へのウェブ・インタフェースが一切存在しないその他の同報通信モデルも設計することができる。このモデルでは、エンドユーザ装置１０９（すなわち、ＩＲＤ）に同報通信送達するためにプロモーション・コンテンツが特別にフォーマットしたディジタル・ストリームにパッケージ化され、そこではストリームをデコードし、そこから購入選択を行うことができるプロモーション・コンテンツをエンドユーザに提示するために特別な処理が行われる。

【０３１４】実際の購入選択は、依然として、エンドユーザ装置１０９からクリアリング・ハウス１０５へのバック・チャネル通信により開始され、ＳＣを使用してすべてのデータ交換を実行することになるだろう。電子ディジタル・コンテンツ・ストア１０３に提供されたツールセットは、そのツールのほとんどがポイントツーポイント・インターネット・サービス・オファリングならびに同報通信衛星またはケーブル・オファリングの両方に適用されるように設計され開発されている。コンテンツ１１３を取得して管理すると同時にＳＣを作成するためにディジタル・コンテンツ・ウェブ・サイトの電子ディジタル・コンテンツ・ストア１０３が使用するツールは、同報通信インフラストラクチャ上での配布のためにコンテンツ１１３を管理し作成するために衛星ベースの電子ディジタル・コンテンツ・ストア１０３も使用する。ウェブ・サービスにより配布されるＳＣは、同報通信サービスにより配布されるものと同じである。

【０３１５】１．マルチティア・ディジタルＴＶの実施形態

次に図２２に移行すると、本発明により同報通信インフラストラクチャを使用するディジタル・コンテンツの電子配布の代替実施形態を示す高レベル論理図が示されている。この実施形態では、図９で前述したように、コンテンツ・プロバイダ１０１は１つまたは複数の電子ディジタル・コンテンツ・ストア１０３にメタデータＳＣ６２０を提供し、１つまたは複数のコンテンツ・ホスト・サイト１１１にコンテンツＳＣ６３０を提供する。電子ストア１０３はメタデータＳＣ６２０をカストマイズしてオファーＳＣ６４１を作成した。オファーＳＣ６４１は１つまたは複数の同報通信センタ１８０２に送られる。そのうえ、メタデータＳＣ６２０に対応するコンテンツＳＣ６３０は１つまたは複数のコンテンツ・ホスト１１１から同報通信センタ１８０２に送られる。オファーＳＣ６４１は衛星、ケーブル、DirectTV、その他の同報通信メカニズムなどの同報通信インフラストラクチャにより１つまたは複数のエンドユーザ装置１０９に送られる。この実施形態では、エンドユーザ装置１０９はテレビのディスプレイ１８０６とセットトップ・ボックス１８０４に結合されている。ただし、セットトップ・ボックス１８０４およびエンドユーザ装置１０９は論理的かつ物理的に互いに異なる装置または１つの装置にすることができることに留意されたい。エンドユーザ装置１

０９は、電話回線などのバック・チャネルによりクリアリング・ハウス１０５への定期接続を行う。

【０３１６】図２３は、図２２の詳細ブロック図であり、本発明により同報通信インフラストラクチャを使用するディジタル・コンテンツの電子配布の代替実施形態を示している。同報通信センタ１８０２はオファーＳＣ６４１を受け取る。カルーセル・ビルダ＆ブロードキャスタ１９０２は、同報通信ストリームとともに送られる様々な追加の同報通信コンテンツを作成する。１次同報通信ストリームとともにディジタル情報またはディジタル・コンテンツを伝送するための技法としては、標準のテレビ放送の垂直帰線消去期間に情報を入れるIntelのIntellicastシステムを含む。他の実施形態では、この情報は同報通信伝送用のＭＰＥＧ－２標準トランスポート・ストリームとして送ることができ、これにより、実質的にすべてのタイプのディジタル同報通信システムによりこのソリューションを配備することができる。図２４は、本発明により図２２の代替実施形態で同報通信されるパケットのブロック図である。オファーＳＣ６４１は、コンテンツＳＣ６３０およびグローバルＳＣ２０４０を含む長さＮの一連のパッケージ２００６に分解され、それはトランザクションＳＣ６４０と類似しているが、対称キー６２３に関して重要な相違点がある。グローバルＳＣの対称キー６２３は、会計情報を調停するためにエンドユーザ装置１０９とクリアリング・ハウス１０５との間で定期接続が行われない場合にコンテンツ１１３を使用不可にするタイムアウト・メカニズムを有する。対称キー６２３にタイムアウト設備を設けることにより、エンドユーザ装置１０９は、まずクリアリング・ハウス１０５と接続する必要なしに、事前定義期間の間、コンテンツ１１３を受け取り、アセンブルし、暗号化解除することができる。期間の１つは、エンドユーザ装置１０９のユーザの１人が月極定期購読料を支払う加入ベースのサービスにすることができるだろう。ユーザが購読料の支払いとクリアリング・ハウス１０５との調停を怠った場合、コンテンツ１１３は使用不可になる。前述のパッケージ２００６に加え、コンテンツＳＣ６３０およびグローバルＳＣ２０４０と、各コンテンツ１１３ごとのトラック２００２が送られる。音楽の実施形態では、トラック２００２は音楽トラックである。パッケージ・フォーマットのカルーセル・フォーマットを図２４に示すが、パッケージ２００６は循環構造内で同報通信インフラストラクチャにより伝送され、定期的に繰返し現れる。循環同報通信の一部はマスタ・カタログ（図示せず）であり、一連のパケット（Ｐ＿１．．．Ｐ＿Ｎ）の一部としてのバグ・カタログはパケット・ストリームの一部として送られる。

【０３１７】前述のように、ディジタル・コンテンツ１１３はパッケージ２００６単位で構成される。１つのパッケージ２００６は、プロモーション素材、メタデータ、パッケージ記述子、１つの（任意選択の）ビデオクリップに関連付けられている。プロモーション素材はパッケージ・ディジタル・コンテンツに関連するグラフィックスおよびテキスト素材からなり（たとえば、音楽アルバムに関連するカバー・アート）、メタデータはそのパッケージに関連する１組の属性値対であり（たとえば、タイトル、価格、アーチストなど）、パッケージ記述子は構造化ディジタル・コンテンツをパッケージから抽出するために使用する１組の属性値対であり（たとえば、パッケージサイズおよびセクション数）、ビデオクリップはそのパッケージのコンテンツをビデオ・フォーマットで提示しプロモーションする（たとえば、そのパッケージに関連する音楽アルバムに含まれる歌曲を演奏するアーチストの短い音楽ビデオ）。

【０３１８】パッケージ２００６ならびにプロモーション素材、ビデオクリップ、メタデータ、パッケージ記述子は、カルーセル方式で１つまたは複数のディジタル同報通信チャネルで同報通信センタ１８０２によって伝送される。カルーセルは、１組の同報通信間隔により繰返し現れる連続ディジタル・ストリームである。同報通信受信機により、ユーザはパッケージ２００６を選択してダウンロードすると同時にディジタル・コンテンツをパッケージから抽出することができる。

【０３１９】パッケージ２００６は、静的オファリング（図示せず）と動的オファリング（図示せず）という２つのセットに構成されている。静的オファリングはアクティブ・パッケージ２００６、すなわち、現在カルーセルで同報通信されているパッケージ２００６のセットを表す。動的オファリングは、サーバ側で使用可能であり、現在同報通信されていないパッケージ２００６のセットを表す。次に静的オファリング・セットは、ビデオクリップ静的オファリングとビデオカタログ静的オファリングという２つのサブセットに構成されている。ビデオ・クリップ静的オファリングはアクティブ・ビデオ・クリップを有するパッケージ２００６のセットを表し、ビデオ・カタログ静的オファリングはアクティブ・ビデオ・クリップを持たないパッケージ２００６のセットを表す。

【０３２０】以下の「Ｘ．エンドユーザ装置」の項で詳述するように、セットトップ・ボックス１８０４上で実行されるアプリケーションは、ビデオ・デコーダ、グラフィカル・ユーザ・インタフェースを提供し、ユーザ入力を受け取る。セットトップ・ボックス１８０４により、ユーザはディジタルＴＶチャネルにチューニングして、ビデオクリップ静的オファリングに関連するビデオ・クリップを表示することができる。また、セットトップ・ボックス１８０４により、ユーザは、静的オファリング・セットと動的オファリング・セットの両方からダウンロードするためのパッケージ２００６を選択することができる。ユーザは、表示された適切なアイコンを選

択することにより、ビデオクリップ静的オファリング・パッケージ２００６を選択してダウンロードし、各パッケージ２００６に関連するビデオ・クリップはセットトップ・ボックス１８０４によって再生される。ユーザは、（１）静的オファリング・カタログを表示するアイコン（すなわち、このセットで使用可能なパッケージ２００６のアイコン・ベースの図形表現）を選択し、（２）所望の選択を突き止めるためにカタログをナビゲートし、（３）所望のパッケージを選択することにより、ビデオカタログ静的オファリングを選択してダウンロードする。セットトップ・ボックス１８０４は同報通信センタ１８０２と通信して、この動的オファリング・パッケージの同報通信を要求する。同報通信センタ１８０２は、ユーザのセットトップ・ボックス１８０４からすべての要求を収集し、カルーセルにパッケージ２００６を割り当て、同報通信間隔にカルーセルを割り当てるスケジューリング・アルゴリズムを実施する。動的オファリング・パッケージがカルーセルに割り当てられると（したがって、同報通信間隔に割り当てられると）、それは静的オファリング・パッケージになる。

【０３２１】すべてのパッケージ２００６、プロモーション素材、メタデータ、記述子がマスタ・カタログ内で収集される。マスタ・カタログは事前設定カルーセルで同報通信される。静的オファリング・セットに属すパッケージ２００６はバグ・カタログにリストされる。バグ・カタログは以下のものを含む。

・　静的オファリング・セットでパッケージを受け取るために必要な同報通信アドレス指定およびチューニング情報
・　ビデオ・クリップを受け取るための同報通信アドレス指定情報
・　マスタ・カタログを受け取るために必要な同報通信アドレス指定情報
・　現在同報通信されているビデオ・クリップに関連するパッケージを指し示すポインタ
・　静的オファリング・セットに属すパッケージ２００６を表すポインタのセット
・　マスタ・カタログ・バージョン
・　バグ・カタログ・バージョン

バグ・カタログはポインタのみを含むので、非常に小型であり、頻繁に更新しダウンロードすることができる。このようにして、セットトップ・ボックス１８０４は同報通信チャネルの状態によってしきりに更新することができる。

【０３２２】グラフィカル・ユーザ・インタフェースを構築し表すために、セットトップ・ボックス１８０４はマスタ・カタログをダウンロードし、含まれるデータを抽出する。選択したパッケージをダウンロードするために、セットトップ・ボックス１８０４は、そのパッケージを含むカルーセルにチューニングし、そのパッケージに関連するデータの収集を開始する。パッケージ・データはセクション単位で構成されている。ディジタル伝送エラーにより、セクションは破壊されたり喪失される場合がある。セクションの完全性はＣＲＣ－３２スタイル情報を使用して判定される。一実施形態では、セットトップ・ボックス１８０４はカルーセル・サイクルによりすべてのパッケージ・セクションを収集する。すべてのセクションが収集され、整理し直されると、セットトップ・ボックス１８０４はそのパッケージを再アセンブルする。個別の両方向ユニキャスト・チャネル（インターネットなど）が使用可能である場合、セットトップ・ボックス１８０４はこのチャネルを使用して、パッケージの欠落部分を収集することができる。後者のメカニズムを使用すると、パッケージ・ダウンロード時間は大幅に削減される。

【０３２３】ビデオクリップ静的オファリング、ビデオカタログ静的オファリング、動的オファリング・セットを構築するために、同報通信センタ１８０２内のストア・マネージャ・アプリケーション（図示せず）を使用する。また、パッケージ２００６をカルーセルに関連付け、各カルーセルおよび各ビデオ・クリップの同報通信間隔を決定するためにも、同じアプリケーションを使用する。同報通信マネージャ・アプリケーションによって実行されるアクションは、同報通信センタ１８０２によってリアルタイムで実施される。

【０３２４】パッケージ記述子およびプロモーション素材は、受信機のリアルタイム更新を可能にする２ティア・パラダイムを使用して同報通信される。

【０３２５】２．個別チャネルによるウェブ同報通信の実施形態

図３１は、図２２の詳細ブロック図であり、本発明によりウェブ同報通信サービス内の個別チャネルを使用するディジタル・コンテンツの電子配布の代替実施形態を示している。図３１のこの例示的なアーキテクチャの概要は、同報通信または通信回線による音楽コンテンツの送達のために他の実施形態から加える必要がある少数の変更を例示するために使用したものである。特に、Hughs DirecPCTMなどの現行のウェブキャスト・インフラストラクチャを使用すると、エンドユーザ装置１０９に関して以下に詳述するように、既存のHughs DirecPCTMシステムとともに機能するように本システムの実施形態のみを適合させるために、トリガ・マネージャ２７２６など、数個の要素しか追加されない。

【０３２６】前述のように、同報通信センタ２７０２は、電子ディジタル・コンテンツ・ストア１０３からオファーＳＣ６４１を受け取る。オファーＳＣ６４１とともに、対応するコンテンツＳＣ６３０が取り出される。この実施形態では、オファーＳＣ６４１およびコンテンツＳＣ６３０がコンピュータ記憶装置２７０４にローカルに記憶される。ＣＧＩまたはサーブレット・スクリプ

ト２７０８および２７１０を実行するウェブ・ストア２７０６は、プロモーション・コンテンツを取得して、図３２に示し以下に詳述するようにサンプル・ボタンおよびカタログ・リストを形成する。クレジット・カード、デビット・カード、その他の支払検証システムなどの支払認証を処理するために、ｅコマースＣＧＩ２７１０は金融クリアリング・ハウス２７１０とのインタフェースを取る。ウェブ・ストア２７０６上に置かれたコンテンツはリポジトリ２７１２に送られる。

【０３２７】一実施形態では、リポジトリに送られるコンテンツは、バック・チャネルを介してエンドユーザ装置１０９から受け取ったユーザ選択に応答するものである。したがって、この実施形態では、エンドユーザ装置１０９から生じた需要と一致するようにコンテンツをスケジューリングすることができる。そのうえ、より人気のあるユーザ選択がより頻繁に同報通信される場合、リポジトリ２７１２に送られるコンテンツの周期性を変更することができる。

【０３２８】オファーＳＣ６４１およびコンテンツＳＣは、様々なチャネル全域で送信機２７１６による同報通信用に選択される。一実施形態では、サーバ／クローラ２７１４は、「ウェブ・クローリング」として知られる技法を使用して、伝送すべきコンテンツを取り出すが、その場合、クローラはＵＲＬなどの識別子またはその他の何らかの検索プロセスによりコンテンツ参照を自動的かつ再帰的に取り出す。他の実施形態では、電子ディジタル・コンテンツ・ストア１０３は、オファーＳＣ６４１およびコンテンツＳＣ６３０に入れて実施されたコンテンツを「プッシュ」することができる。コンテンツがアセンブルされると、送信機２７１６は１つまたは複数の選択チャネル上でオファーＳＣ６４１を伝送し、他のチャネル上で対応するコンテンツＳＣを伝送する。送信機はDirecPCTMまたは互換性のあるトランシーバである。コンテンツＳＣ６３０は、個別のダウンロード・チャネル上でそれぞれ同報通信されるようにパッケージ化することができる。同報通信用の全使用可能通信帯域幅はすべてのチャネルによって共用される。多数のチャネルを有する同報通信システムでは、特定のタイトルまたは選択用の各コンテンツＳＣ６３０は、個別チャネルで同報通信することができる。このスケジュールは、各チャネルごとに特定の周期性を保証するように静的に設計することができる。この設計では、非常に人気のあるコンテンツを１つまたは複数のチャネル上でより頻繁に同報通信することができる。電話回線またはネットワークなどのバック・チャネルが存在する場合、同報通信コンテンツはユーザ選択に基づいて動的にスケジューリングされる。

【０３２９】一実施形態では、オファーＳＣ６４１内のプロモーション素材は、ＳＣから取り出され、チャネルにより伝送される。プロモーション素材をＳＣ内に保持する必要性は、そのプロモーション素材によって決まる。

【０３３０】エンドユーザ装置１０９は、受信機１８０４により同報通信を受信する。直接同報通信実施形態の受信機２７１８は、DirecPCTM用パラボラアンテナまたはDirecPCTM／DirectTVTM兼用パラボラアンテナあるいはそれと同等のウェブ・キャスト同報通信システムに結合されたＵＳＢモデムである。キャッシュ・マネージャ２７２０は、エンドユーザ装置１０９でのコンテンツおよびプロモーション素材のダウンロードを管理するソフトウェア・プログラムである。プロモ・キャッシュ２７２２およびアルバム＋ＤＳＣバッファ２２２４という２つのリポジトリが示されている。これらは、エンドユーザ装置１０９内の２つの別々の記憶領域として示されているが、これらのリポジトリ２７２２および２７２４をより多くの記憶領域にさらに分割するか、エンドユーザ装置上の単一記憶領域に結合することができることは当業者には明白になるだろう。しかも、エンドユーザ装置１０９内の多くのコンポーネントは、１つのユニットに結合するか、受信機２７１８、キャッシュ・マネージャ２７２０、ウェブ・ブラウザ１９１、プロモ・キャッシュ２７２２、アルバム＋ＤＳＣバッファ２７２４を含む個別ハードウェアとして実現することができる。たとえば、一実施形態のDirecPCTMはセットトップ・ボックス１８０４に収容される。

【０３３１】ＤＳＣという用語の使い方に留意することは重要である。ＤＳＣは、「切断ＳＣ」の省略形である。これはコンテンツＳＣ６３０と同一であるが、接頭部「Ｄ」はこの実施形態では、エンドユーザ装置が切断されたとき、すなわち、送信機２７１６から同報通信を受信していないか、バック・チャネルによりウェブ・ストア２７０６に返信していないか、あるいはその両方の場合でも、エンドユーザ装置１０９上でローカルにコンテンツＤＳＣを取り出すことができることを強調するために使用している。

【０３３２】前述のように、プロモ・キャッシュ２７２２はエンドユーザ装置１０９が受信したプロモーションを記憶し、同様にアルバム＋ＤＳＣ２７２４はコンテンツＳＣ６４１を記憶する。プロモーション・チャネルに加入しているユーザの場合、プロモ・キャッシュ２７２２に記憶されたプロモーション素材またはオファーＳＣ６４１は、プロモーション・パッケージの新バージョンが同報通信されたときに必ず更新される。プロモーション・コンテンツを最新の状態に保持することにより、ユーザは、オフラインでブラウズしているときにプロモーション・コンテンツが最も最新のものになるよう保証される。より大型のアルバム＋ＤＳＣバッファ２７２４を備えたシステムでは、プロモーション素材が更新されたときに、対応するコンテンツＳＣ６３０が記憶され更新される。コンテンツに関する両方のプロモーション素材

をローカルに記憶すると、コンテンツを含むユーザ・システムが最新のものになる。

【０３３３】ウェブ・ブラウザ１９１を使用するユーザは、プロモ・キャッシュ２７２２に事前にキャッシュされたプロモーション素材をブラウズする。例示的なユーザ・インタフェースは、以下の図３２に示されている。前述のようにプロモーション素材が記憶されているので、同報通信センタ２７０２から同報通信を受信するように「接続」されているか否かにかかわらず、ユーザがプロモーション素材をブラウズできることは留意すべき重要なことである。

【０３３４】一実施形態では、ユーザがプロモーション素材を選択すると、トリガ・マネージャ２７２６によって起動されるプレーヤ・アプリケーション１９６によりサンプル・クリップを再生することができる。ユーザがウェブ・ブラウザ１９１を使用して選択を行うと、キャッシュ・マネージャは、対応するコンテンツＳＣ６３０がアルバム＋ＤＳＣバッファ２７２４内で使用可能になっているかどうかを確認するためのチェックを行い、対応するコンテンツＳＣ６３０がすでにダウンロードされている場合、それはキャッシュ・マネージャに与えられ、トリガ・マネージャ２７２６を起動し、「接続」実施形態のプレーヤ・アプリケーション１９５に関して前述したようにコンテンツＳＣ６３０の処理を開始する。対応するコンテンツＳＣ６３０がアルバム＋ＤＳＣバッファ２７２４で使用可能になっていない場合、キャッシュ・マネージャ２７２０は要求を行う。キャッシュ・マネージャ２７２０に対する要求または加入要求は、コンテンツＳＣ６３０の同報通信用に適切なチャネルを選択するよう受信機を制御する。コンテンツＳＣ６３０用のチャネルは、ダウンロードするプロモーションごとにプロモ・キャッシュ２７２２内の１つのテーブルに記憶することができる。このため、同報通信スケジュールの変更をローカルで追跡することができる。コンテンツＳＣ６３０の次のスケジュール同報通信は、受信機２７１８によって受信され、アルバム＋ＤＣバッファ２７２４にローカルにキャッシュされる。キャッシュ・マネージャ２７２０は、正しい間隔で自動的にウェイクアップしてダウンロードのために対応するチャネルを選択するようにプログラミングすることができる。

【０３３５】任意選択の実施形態では、同報通信センタ２７０２へのインターネットなどのバック・チャネルを使用してユーザが次にサインオンまたはログオンすると、ｅコマース・サイト２７１０を使用してクレジット・カード支払などのユーザ会計情報の確認が行われる。その他の実施形態では、クリアリング・ハウス１０５またはウェブ・ストア２７０６に再接続することなしにユーザが所与の数の購入を行えるようにすることにより、コンテンツ１１３の「オフライン」購入が実施される。この「オフライン」実施形態では、所与の期間または価値据置きの範囲内で再接続が行われるまで、クレジット限界、購入限界、定期接続、コンテンツ１１３の時限使用などのいくつかのカテゴリを使用することができる。

【０３３６】要求された適切なコンテンツＳＣ６３０のスケジューリングおよびダウンロードをキャッシュ・マネージャ２７２０が完了すると、トリガ・マネージャ・アプリケーション２７２６はプレーヤ・アプリケーション１９５に通知し、コンテンツはアルバム＋ＤＳＣバッファ２７２４からプレーヤ・アプリケーション１９５へのインポートに使用可能になる。コンテンツＳＣがダウンロードされたことをプレーヤ・アプリケーションに通知することに加え、ダウンロードの状況、ダウンロード時のエラー、所望のコンテンツ１１３を演奏または再生したいと希望する際にユーザにとって有用なその他の情報などのその他の状況をキャッシュ・マネージャ２７２０からプレーヤ・アプリケーション１９５に報告することができる。

【０３３７】現行の送達システムの「オンライン」または「接続」バージョンについて前述したように、コンテンツに関連する使用条件および権利を更新するために必要なステップはクリアリング・ハウス１０５によって監視することができる。

【０３３８】Ｘ．エンドユーザ装置１０９

セキュア・ディジタル・コンテンツ電子配布システム１００用のエンドユーザ装置１０９におけるアプリケーションは、第１にＳＣの処理およびコピー制御と、第２に暗号化コンテンツ１１３の再生という２つの主な機能を果たす。エンドユーザ装置１０９は、パーソナル・コンピュータであるか専用の電子消費者装置であるかにかかわらず、これらの基本機能を実行できなければならない。また、エンドユーザ装置１０９は、再生リストの作成、ディジタル・コンテンツ・ライブラリの管理、コンテンツ再生中の情報および画像の表示、外部媒体装置への記録のような様々な追加機構および機能も提供する。このような機能は、これらのアプリケーションがサポートするサービスと、これらのアプリケーションの設計対象である装置のタイプに基づいて様々である。

【０３３９】Ａ．概要

次に図１３を参照すると、主要コンポーネントおよびプロセスと、エンドユーザ装置１０９の機能フローが示されている。ＰＣベースのウェブ・インタフェース・コンテンツ１１３のサービスをサポートするように設計されたアプリケーションは、ＳＣプロセッサ１９２とプレーヤ・アプリケーション１９５という２通りの実行可能ソフトウェア・アプリケーションからなる。ＳＣプロセッサ１９２は、ＳＣファイル／ＭＩＭＥタイプを処理するためにエンドユーザのウェブ・ブラウザ１９１内にヘルパ・アプリケーションとして構成された実行可能アプリケーションである。このアプリケーションは、電子ディジタル・コンテンツ・ストア１０３、クリアリング・ハ

ウス１０５、コンテンツ・ホスト・サイト１１１からＳＣを受け取ったときに必ずブラウザによって立ち上げられる。これは、ＳＣに関するすべての必須処理を実行し、最終的にコンテンツ１１３をエンドユーザのディジタル・コンテンツ・ライブラリ１９６に追加することを担当する。

【０３４０】プレーヤ・アプリケーション１９５は、自分のディジタル・コンテンツ・ライブラリ１９６内のコンテンツ１１３を実行し、自分のディジタル・コンテンツ・ライブラリ１９６を管理し、許されるならばコンテンツ１１３のコピーを作成するためにエンドユーザがロードするスタンドアロンの実行可能アプリケーションである。プレーヤ・アプリケーション１９５とＳＣプロセッサ１９２の両方のアプリケーションは、Java、Ｃ／Ｃ＋＋、またはそれと同等のソフトウェアで作成することができる。好ましい実施形態では、ウェブサイトなどのコンピュータ可読手段からアプリケーションをダウンロードすることができる。しかし、ディスケットまたはＣＤなどのコンピュータ可読手段で送達するなど、その他の送達メカニズムも可能である。

【０３４１】コンテンツ１１３の情報のサーチおよびブラウズ、たとえば歌曲クリップのプリビュー、購入用の歌曲の選択は、いずれもエンドユーザのウェブ・ブラウザ１９１により処理される。電子ディジタル・コンテンツ・ストア１０３は、多くのコンテンツ１１３小売ウェブ・サイトにより今日提供されるものと同じ方法でショッピング経験を提供するものである。エンドユーザにとって今日のウェブ・ベースのコンテンツ１１３ショッピングを上回る相違点は、自分のショッピング・カートに追加すべきダウンロード可能なコンテンツ１１３のオブジェクトを選択できることである。電子ディジタル・コンテンツ・ストア１０３がダウンロード可能なオブジェクトに加え販売用に使用可能なその他の商品を有する場合、エンドユーザは自分のショッピング・カート内に物理的商品とダウンロード可能な電子商品との組合せを有することができる。エンドユーザがチェックし、自分の最終購入許可を電子ディジタル・コンテンツ・ストア１０３に提示するまで、セキュア・ディジタル・コンテンツ電子配布のエンドユーザ装置１０９は関わりがない。この時点の前のすべての対話は、電子ディジタル・コンテンツ・ストア１０３用のウェブ・サーバとエンドユーザ装置１０９上のブラウザ１９１との間で行われる。これは、サンプル・ディジタル・コンテンツ・クリップのプリビューを含む。ディジタル・コンテンツ・クリップはＳＣ内にパッケージ化されないが、むしろ、ダウンロード可能なファイルとして電子ディジタル・コンテンツ・ストア１０３のウェブ・サービスに統合されるかまたはストリーミング・サーバから供給される。コンテンツ１１３クリップのフォーマットはシステム・アーキテクチャによって指示されない。他の実施形態では、プレーヤ・アプリケーション１９５が電子ディジタル・コンテンツ・ストア１０３またはクリアリング・ハウス１０５と直接対話するか、あるいはプロモーションＣＤを使用してオフラインで対話することができるだろう。

【０３４２】Ｂ．アプリケーションのインストール

プレーヤ・アプリケーション１９５とヘルパ・アプリケーション１９８１は、多くのウェブ・サイトからダウンロード用に使用可能な自己インストール実行可能プログラムにパッケージ化される。クリアリング・ハウス１０５は、パブリック・ウェブ・サイトにあるマスタ・ダウンロード・ページのホストとなる中央位置として動作する。これは、そこからインストール・パッケージをダウンロードすることができる位置へのリンクを含む。このインストール・パッケージは、ダウンロード要求の地理的分散を可能にするためにすべてのコンテンツ・ホスト・サイト１１１で入手可能である。各参加電子ディジタル・コンテンツ・ストア１０３もそのサイトからのダウンロード用にそのパッケージを使用可能な状態にすることができる場合もあれば、クリアリング・ハウス１０５のパブリック・ウェブ・サイトにあるマスタ・ダウンロード・ページへのリンクを提供するだけの場合もある。

【０３４３】ダウンロード可能なコンテンツ１１３を購入したいと希望するエンドユーザは、このパッケージをダウンロードしてインストールする。このインストールは、このダウンロード可能なパッケージ内で独立したものである。これは、ヘルパ・アプリケーション１９８とプレーヤ・アプリケーション１９５の両方をアンパックしてインストールし、インストールされたウェブ・ブラウザに応じてヘルパ・アプリケーション１９８の構成も行う。

【０３４４】インストールの一部として、オーダおよびライセンスＳＣ６６０を処理する際に使用するためにエンドユーザ装置１０９用に公開／秘密キー６６１の対が作成される。ライセンス・データベース１９７内の歌曲暗号化キーを保護する際に使用するためにランダム対称キー（機密ユーザ・キー）も生成される。この機密ユーザ・キー（図示せず）は、そのキーを複数のパーツに分解し、そのキーのピースをエンドユーザのコンピュータ全体の複数の位置に記憶することによって保護される。このコードの領域は、そのキーがどのようにセグメント化され、どこに記憶されているかを漏らさないように改竄防止ソフトウェア技術によって保護される。エンドユーザによるこのキーへのアクセスすら防止することにより、その他のコンピュータとのコンテンツ１１３の共用または著作権侵害を防止するのに役に立つ。これらのキーの使い方の詳細についてはＳＣプロセッサ１９２の項を参照されたい。

【０３４５】改竄防止ソフトウェア技術は、ハッカによるコンピュータ・ソフトウェア・アプリケーションへの無許可侵入を阻止するための方法である。通常、ハッカ

はソフトウェアを理解したいと希望するか、ソフトウェアを変更してその使用に関する制限を除去したいと希望するものである。特に、侵入できないコンピュータ・プログラムはまったく存在せず、これが改竄防止ソフトウェアが「耐改竄性」と呼ばれない理由である。しかし、改竄防止保護アプリケーションに侵入するのに必要な労力は得られる利益に値しないので、通常、ほとんどのハッカを阻止することになる。この場合、その労力はコンテンツ１１３の１つのピース、おそらくＣＤ上の１つの歌曲へのキーにアクセスすることになるだろう。

【０３４６】１つのタイプの改竄防止ソフトウェア技術はＩＢＭから得られる。このコードが導入された製品の１つは、ＩＢＭのThinkPad770ラップトップ・コンピュータに内蔵されている。この場合、改竄防止ソフトウェアはコンピュータ内のＤＶＤ映画プレーヤを保護するために使用された。ハリウッド・スタジオなどのディジタル・コンテンツ・プロバイダは、ディジタル映画の出現と完璧なコピーを作成できる容易さを懸念し、ＤＶＤディスク上の映画がコピー保護メカニズムを含むべきだと主張してきた。ＩＢＭの改竄防止ソフトウェアは、このようなコピー保護メカニズムを回避しにくくするものである。これは改竄防止ソフトウェアにとって非常に典型的な応用例であり、このソフトウェアを使用して、何らかの保護タイプのコンテンツ１１３の使用に関する規則を施行する。

【０３４７】ＩＢＭの改竄防止ソフトウェアは、攻撃者の経路にいくつかのタイプの障害物を置くものである。第１に、それはハッカが使用する標準的なソフトウェア・ツール、すなわち、デバッガおよび逆アセンブラを無効にするかまたは少なくともその効力を低減するための技法を含む。第２に、それは自己完全性チェックを含むので、単一変更またはほんの少数の変更でも検出され、間違った動作を引き起こすことになる。最後に、それは、その本当の動作に関してハッカを誤解させるための不明化部分を含む。後者の技法は主として特定の問題のみに関するものであるが、最初の２つは暗号化およびディジタル・シグニチャという暗号化技術で周知のツールに基づくものである。

【０３４８】Ｃ．セキュア・コンテナ・プロセッサ１９２

エンドユーザが自分のショッピング・カートに収集した商品について電子ディジタル・コンテンツ・ストア１０３に最終購入許可を提示すると、そのウェブ・ブラウザは、ウェブ・サーバからの応答を待ってアクティブなままになる。電子ディジタル・コンテンツ・ストア１０３のウェブ・サーバは、その購入を処理し、金融決済を実行し、トランザクションＳＣ６４０をエンドユーザ装置１０９に返す。トランザクションＳＣ６４０に関連するＳＣＭＩＭＥタイプを処理するために、ウェブ・ブラウザによってＳＣプロセッサ１９２（ヘルパ・アプリケーション１９８）が立ち上げられる。図１７は、本発明により図１３に記載するようにローカル・ライブラリにコンテンツをダウンロードするプレーヤ・アプリケーション１９５のユーザ・インタフェース画面の一例である。

【０３４９】ＳＣプロセッサ１９２は、トランザクションＳＣ６４０をオープンし、そこに含まれるオファーＳＣ６４１と応答ＨＴＭＬページを抽出する。応答ＨＴＭＬページはエンドユーザの購入を確認するブラウザ・ウィンドウに表示される。次にステップ１４０１でオファーＳＣ６４１がオープンされ、予定ダウンロード時間とともにコンテンツ１１３（たとえば、歌曲またはアルバム）の名前がそこから抽出される。次にステップ１４０２でこの情報を含む新しいウィンドウが表示され、コンテンツ１１３のダウンロードをスケジューリングするためのオプション（たとえば、音楽の場合は複数歌曲またはアルバム全体）がエンドユーザに提示される。エンドユーザは即時ダウンロードを選択するかまたはダウンロードを後で行うようにスケジューリングすることができる。後で行うことを選択した場合、ダウンロード・スケジュール情報がログに保管され、エンドユーザ装置１０９がその予定時間に電源投入された場合にその時点でダウンロードが開始される。その予定ダウンロード時間にコンピュータがアクティブになっていないかまたは通信リンクがアクティブになっていない場合、エンドユーザは、コンピュータが次に電源投入されたときにダウンロードのスケジューリングをやり直すよう要求される。

【０３５０】予定ダウンロード時間が発生するかまたは即時ダウンロードが要求された場合、ＳＣプロセッサ１９２は、トランザクションＳＣ６４０、オファーＳＣ６４１、インストール時に作成されたエンドユーザの公開キー６６１内の情報からオーダＳＣ６５０を作成する。このオーダＳＣ６５０はＨＴＴＰ要求によりクリアリング・ハウス１０５に送られる。クリアリング・ハウス１０５がライセンスＳＣ６６０を返すと、ライセンスＳＣ６６０を処理するためにヘルパ・アプリケーション１９８が再呼出しされる。次にライセンスＳＣ６６０がオープンされ、参照したオーダＳＣ６５０からコンテンツ・ホスト・サイト１１１のＵＲＬが抽出される。次にコンテンツＳＣ６３０のダウンロードを要求するブラウザによるhttp要求によって、ライセンスＳＣ６６０が指定のコンテンツ・ホスト・サイト１１１に送られる。コンテンツＳＣ６３０がブラウザに戻ると、ヘルパ・アプリケーション１９８がもう一度、再呼出しされる。ＳＣプロセッサ１９２は、ダウンロード経過インジケータおよび推定完了時間とともにダウンロード中のコンテンツ１１３の名前を表示する。

【０３５１】ＳＣプロセッサ１９２によってコンテンツ１１３が受信されると、それは暗号化解除のためにコンテンツ１１３のデータをメモリ・バッファにロードする。バッファのサイズは、暗号化アルゴリズムとウォー

タマーク技術１９３の要件によって決まり、ハッカ・コードに曝される未暗号化コンテンツ１１３の量を低減するために可能な最小サイズになっている。バッファがいっぱいになると、それはライセンスＳＣ６６０から抽出したエンドユーザのキー６２３（公開キー６６１に対応するもの）を使用して暗号化解除されるが、それ自体はまず秘密キーを使用して暗号化解除される。次に、暗号化解除したバッファがウォータマーク機能に渡される。

【０３５２】ウォータマーク１９３は、ライセンスＳＣ６６０からウォータマーク命令を抽出し、エンドユーザの秘密キーを使用してその命令を暗号化解除する。次にウォータマーク・データは、そこからこのコンテンツ１１３が購入された電子ディジタル・コンテンツ・ストア１０３に登録された購入者の名前などのトランザクション情報を含むライセンスＳＣ６６０から抽出されるか、あるいは電子ディジタル・コンテンツ・ストア１０３が登録機能を提供しない場合はクレジット・カード登録情報から導出される。また、ウォータマークには、購入日と、このトランザクションに関してログ記録された特定のレコードを参照するために電子ディジタル・コンテンツ・ストア１０３が割り当てたトランザクションＩＤ５３５も含まれる。また、プレーヤ・アプリケーション１９５のコピー制御が使用するためにストア使用条件５１９も含まれる。

【０３５３】ウォータマーク１９３は、ウォータマーク命令を漏らさないように改竄防止コード技術によって保護され、したがって、ハッカがウォータマークの位置および技法を発見するのを防止する。これにより、ハッカによるウォータマークの除去または変更が防止される。

【０３５４】このコンテンツ・バッファに必須ウォータマークを銘記した後、そのバッファは再暗号化１９４用のスクランブル機能に渡される。ＩＢＭのＳＥＡＬ暗号化技術などのプロセッサ有効セキュア暗号化アルゴリズムを使用して、ランダム対称キーによりコンテンツ１１３を再暗号化する。ダウンロード、暗号化解除、再暗号化１９４のプロセスが完了すると、本来コンテンツ１１３を暗号化するためにコンテンツ・プロバイダ１０１が使用した暗号化キー６２３はこの時点で破壊され、インストール時に作成され隠された機密ユーザ・キーを使用して新しいＳＥＡＬキー自体が暗号化される。次にこの新しい暗号化ＳＥＡＬキーはライセンス・データベース１０７に記憶される。

【０３５５】コンテンツ・プロバイダ１０１側で実行される異なるソース、および、エンドユーザ装置１０９側で実行されるユーザ・ウォータマークは、効果的であるために業界標準になる必要があるであろう。このような標準は依然として進化している。この技術は、制御信号を音楽に埋め込み、何回も更新できるようにするために使用可能なものである。コピー制御標準がより安定したものになる時点まで、セキュア・ディジタル・コンテンツ電子配布システム１００には代替コピー制御方法が設けられていたので、消費者装置内で権利管理を可能にするためにコピー制御ウォータマークをあてにしない。記憶および再生／記録使用条件のセキュリティは、エンドユーザ装置１０９に結合された暗号化ＤＣライブラリ・コレクション１９６を使用して実現され、改竄防止環境によって保護される。ソフトウェア・フックは、標準が採用されたときにコピー制御ウォータマークをサポートするために所定の位置にある。現在、様々な圧縮レベルでのウォータマークＡＡＡおよびその他のコード化オーディオ・ストリームのサポートが存在するが、この技術はコピー制御の単独方法として利用するにはこの時点では依然としていくらか時期尚早である。

【０３５６】暗号化解除および再暗号化１９４のプロセスは、元のコンテンツ１１３の暗号化キー、新しいＳＥＡＬキー、機密ユーザ・キー、機密ユーザ・キーのセグメントがどこに記憶されるか、そのキーがどのようにセグメント化されるかを漏らさないように改竄防止コード技術によって保護される、もう１つのコード領域である。

【０３５７】暗号化解除および再暗号化１９４のプロセスは２つの目的に対応する。ＳＥＡＬのようなアルゴリズムによって暗号化されたコンテンツ１１３を記憶するとリアルタイム暗号化解除より高速になり、ＤＥＳのようにより業界標準タイプのアルゴリズムを実行する場合より暗号化解除を実行するのに必要なプロセッサ使用率がかなり低下する。これにより、プレーヤ・アプリケーション１９５は、デコードおよび再生の前にコンテンツ１１３用のファイル全体を先に暗号化解除する必要なしに、コンテンツ１１３のリアルタイム同時暗号化解除デコード再生を実行することができる。ＳＥＡＬアルゴリズムおよび非常に効率の良いデコード・アルゴリズムの効率により、同時動作（暗号化ファイルからのストリーミング再生）が可能になるだけでなく、かなり低電力のシステム・プロセッサ上でこのプロセスを行うこともできる。したがって、このアプリケーションは、６０ＭＨｚのPentiumシステムおよびそれ以下程度のローエンドのエンドユーザ装置１０９上でサポートすることができる。コンテンツ１１３が最終的に記憶される暗号化フォーマットを元の暗号化フォーマットから分離すると、元のコンテンツ暗号化アルゴリズムの選択の際に柔軟性の増大が可能になる。したがって、広く受け入れられ立証された業界標準アルゴリズムを使用することができ、その結果、ディジタル・コンテンツ業界によるセキュア・ディジタル・コンテンツ電子配布システム１００の容認がさらに強化される。

【０３５８】この暗号化解除および再暗号化１９４のプロセスの第２の目的は、このコンテンツ１１３を暗号化するためにコンテンツ・プロバイダ１０１が使用した元のマスタ暗号化キー６２３はこのコンテンツ１１３のラ

イセンスを許諾したすべてのエンドユーザ装置１０９上に記憶しなければならないという要件を除去することである。ライセンスＳＣ６６０の一部としての暗号化マスタキー６２３は、非常に短時間の間、エンドユーザ装置１０９のハード・ディスク上にキャッシュされるだけであり、メモリ内でのみ非常に短時間の間、平文になる。この実行フェーズ中、キー６２３は改竄防止コード技術により保護される。この暗号化解除および再暗号化１９４のフェーズが完了すると、エンドユーザ装置１０９上でいずれかの形式でこのキー６２３を保持する必要はなくなるので、ハッカによる著作権侵害の可能性は大幅に軽減される。

【０３５９】歌曲は、再暗号化されると、ディジタル・コンテンツ・ライブラリ１９６に記憶される。プレーヤ・アプリケーション１９５が使用するために必要なすべてのメタデータは関連オファーＳＣ６４１から抽出され、ステップ１４０３でディジタル・コンテンツ・ライブラリ１９６にも記憶される。歌曲の歌詞など、暗号化されたメタデータのいずれかの部分は、他のコンテンツに関して前述したのと同じように暗号化解除され再暗号化される。暗号化が必要な関連メタデータには、コンテンツ１１３を暗号化するために使用したのと同じＳＥＡＬキーを使用する。

【０３６０】Ｄ．プレーヤ・アプリケーション１９５

１．概要

セキュア・ディジタル・コンテンツ電子配布プレーヤ・アプリケーション１９５（ここではプレーヤ・アプリケーション１９５という）は、ＣＤ、ＤＶＤ、その他のディジタル・コンテンツ・プレーヤと、ＣＤ、ＤＶＤ、その他のディジタル・コンテンツ記憶管理システムの両方に類似したものである。これは、その最も単純なレベルでは、歌曲またはビデオの再生など、コンテンツ１１３を実行する。他のレベルでは、自分のディジタル・コンテンツ・ライブラリ１９６を管理するためのツールをエンドユーザに提供する。まさに重要なことに、歌曲などのコンテンツのコレクション（ここでは再生リストという）の編集および再生を可能にする。

【０３６１】プレーヤ・アプリケーション１９５は、個々に選択し、コンテンツ・プロバイダ１０１および電子ディジタル・コンテンツ・ストア１０３の要件に応じてカストマイズ可能なコンポーネントの集合からアセンブルされる。このプレーヤの汎用バージョンについて説明するが、カストマイズは可能である。

【０３６２】次に図１８および図１９を参照すると、図１３のエンドユーザ装置１０９上で実行されるプレーヤ・アプリケーション１９５の主要コンポーネントおよびプロセスのブロック図が示されている。

【０３６３】プレーヤ・オブジェクト・マネージャ１５０１のサブシステムを構成するコンポーネントセットがいくつか存在する。

１．エンドユーザ・インタフェース・コンポーネント１５０９

２．コピー／再生管理コンポーネント１５０４

３．暗号化解除１５０５、圧縮解除１５０６、再生１５０７の各コンポーネント、記録を含むことができる

４．データ管理１５０２およびライブラリ・アクセス１５０３の各コンポーネント

５．アプリケーション間通信コンポーネント１５０８

６．その他の各種（インストールなど）コンポーネント

【０３６４】これらの各セット内から以下の要件に基づいてコンポーネントを選択することができる。

・　プラットフォーム（Ｗｉｎｄｏｗｓ（登録商標）、ＵＮＩＸ（登録商標）、それと同等のもの）

・　通信プロトコル（ネットワーク、ケーブルなど）

・　コンテンツ・プロバイダ１０１または電子ディジタル・コンテンツ・ストア１０３

・　ハードウェア（ＣＤ、ＤＶＤなど）

・　クリアリング・ハウス１０５の技術など

【０３６５】以下の各項は様々なコンポーネント・セットを詳述するものである。最終項では、これらのコンポーネントがどのように汎用プレーヤに編成されるかを詳述し、そのコンポーネントをどのようにカストマイズできるかを説明する。

【０３６６】他の実施形態では、プレーヤ・アプリケーション１９５およびＳＣプロセッサ１９２のコンポーネントがプログラマのソフトウェア・ツールキットの一部として使用可能になる。このツールキットは、上記の汎用プレーヤ・アプリケーションの各種コンポーネントへの事前定義インタフェースを可能にする。このような事前定義インタフェースは、ＡＰＩまたはアプリケーション・プログラミング・インタフェースの形になっている。このようなＡＰＩを使用する開発者は、各種コンポーネントの機能性のいずれについても高レベル・アプリケーション・プログラムから実現することができる。このようなコンポーネントにＡＰＩを提供することにより、プログラマは、このようなコンポーネントのいずれのついてもその機能およびリソースを再作成する必要なしに、カストマイズしたプレーヤ・アプリケーション１９５を迅速に開発することができる。

【０３６７】２．エンドユーザ・インタフェース・コンポーネント１５０９

このセットからのコンポーネント同士が協力し、プレーヤ・アプリケーション１９５の画面上での発現を可能にする。ただし、設計ではこれらのコンポーネントの決定的なレイアウトを設定していないことに留意されたい。このようなレイアウトの１つは汎用プレーヤに設けられている。コンテンツ・プロバイダ１０１または電子ディジタル・コンテンツ・ストアあるいはその両方からの要件ならびにその他の要件に基づいて、代替レイアウトも可能である。

【０３６８】このセットは、エンドユーザ表示１５１０を提示し、オーディオ再生およびメタデータの提示などの低レベル機能に使用するエンドユーザ・コントロール１５１１というコントロールを扱うために使用するコンポーネントから始まって、複数のサブグループにグループ化される。次にエンドユーザ表示コンポーネント１５１０は特殊機能のグループ化（再生リスト、ディジタル・コンテンツ・ライブラリ）によってさらに分割され、次にオブジェクトコンテナ・コンポーネントはこのような低レベル・コンポーネントのグループ化および配置に使用する。

【０３６９】以下のコンポーネント・リスト内では、ＣＤの作成あるいはＣＤまたはその他の記録可能媒体へのコンテンツ１１３のコピーについて言及した場合、それはプレーヤ・アプリケーション１９５がこのような機能性を使用可能にした場合にのみ適用される。また、その文脈で使用するＣＤという用語は汎用のものであり、ミニディスクまたはＤＶＤなど、その他の様々な記録装置も表すことができることに留意されたい。

【０３７０】図２０は、本発明により図１８ないし図１９のプレーヤ・アプリケーション１９５のユーザ・インタフェース画面の一例である。エンドユーザ・コントロール１５１１用の機能としては以下のものを含む（エンドユーザ・インタフェースの対応画面を１６０１～１６０５として示す）。

コンテンツ１１３を実行するためのコントロール：

・　再生／停止ボタン
・　再生ボタン
・　停止ボタン
・　休止ボタン
・　前進スキップ・ボタン
・　後退スキップ・ボタン
・　ボリューム・コントロール
・　トラック位置コントロール／表示
・　オーディオ・チャネル・ボリューム・レベル表示など

コンテンツ１１３に関連するメタデータを表示するためのコントロール

・　カバー・ピクチャ・ボタン
・　カバー・ピクチャ・オブジェクト
・　アーチスト・ピクチャ・ボタン
・　アーチスト・ピクチャ・オブジェクト
・　トラック・リスト・ボタン
・　トラック・リスト情報オブジェクト
・　トラック・リスト・セレクタ・オブジェクト（クリックして再生）
・　トラック名オブジェクト
・　トラック情報オブジェクト
・　トラック歌詞ボタン
・　トラック歌詞オブジェクト
・　トラック・アーチスト名オブジェクト
・　トラック・クレジット・ボタン
・　トラック・クレジット・オブジェクト
・　ＣＤ名オブジェクト
・　ＣＤクレジット・ボタン
・　ＣＤクレジット・オブジェクト
・　汎用（構成可能）メタデータ・ボタン
・　汎用メタデータ・オブジェクトなど

【０３７１】エンドユーザ表示１５１０用の機能としては以下のものを含む（エンドユーザ・インタフェースの対応画面を１６０１～１６０５として示す）。

表示コンテナの再生リスト

・　再生リスト管理ボタン
・　再生リスト管理ウィンドウ
・　ディジタル・コンテンツ・サーチ・ボタン
・　ディジタル・コンテンツ・サーチ定義オブジェクト
・　ディジタル・コンテンツ・サーチ提示ボタン
・　ディジタル・コンテンツ・サーチ結果オブジェクト
・　再生リストへの選択サーチ結果項目コピー・ボタン
・　再生リスト・オブジェクト（編集可能）
・　再生リスト保管ボタン
・　再生リスト再生ボタン
・　再生リスト休止ボタン
・　再生リスト再始動ボタン
・　再生リストからのＣＤ作成ボタンなどディジタル・コンテンツ・ライブラリ１９６の表示
・　ディジタル・コンテンツ・ライブラリ・ボタン
・　ディジタル・コンテンツ・ライブラリ・ウィンドウ
・　ディジタル・コンテンツ・カテゴリ・ボタン
・　ディジタル・コンテンツ・カテゴリ・オブジェクト
・　アーチスト別ボタン
・　ジャンル別ボタン
・　レーベル別ボタン
・　カテゴリ別ボタン
・　削除ボタン
・　再生リストへの追加ボタン
・　ＣＤへのコピー・ボタン
・　歌曲リスト・オブジェクト
・　歌曲リスト表示コンテナなど

コンテナおよびその他

・　プレーヤ・ウィンドウ・コンテナ
・　オーディオ・コントロール・コンテナ
・　メタデータ・コントロール・コンテナ
・　メタデータ表示コンテナ
・　ツールバー・コンテナ・オブジェクト
・　サンプル・ボタン
・　ダウンロード・ボタン
・　購入ボタン
・　記録ボタン
・　プレーヤ名オブジェクト

・　レーベル／プロバイダ／ストア広告オブジェクト
・　レーベル／プロバイダ／ストアＵＲＬボタン
・　アーチストＵＲＬボタンなど
【０３７２】３．コピー／再生管理コンポーネント１５０４
これらのコンポーネントは、暗号化キーのセットアップ、ウォータマーク処理、コピー管理などを処理する。また、クリアリング・ハウス１０５との通信、購入要求の伝送などのため、ペイパーリッスンなどの特殊サービスまたはコンテンツ１１３にアクセスするごとに課金する場合のためのインタフェースも存在する。現在、クリアリング・ハウス１０５の諸機能への通信はＳＣプロセッサ１９２によって処理されている。
【０３７３】エンドユーザ装置１０９上のプレーヤ・アプリケーション１９５によるコンテンツ１１３の使用は、ライセンス・データベース１９７などのデータベースにログ記録される。プレーヤ・アプリケーション１９５によるコンテンツ１１３の使用ごとの追跡は、クリアリング・ハウス１０５またはコンテンツ・プロバイダ１０１または電子ディジタル・コンテンツ・ストア１０３または指定され伝送インフラストラクチャ１０７に結合された任意のサイトなどの１つまたは複数のログ記録サイトに伝送することができる。この伝送は、ログ記録サイトに使用情報をアップロードするために所定の時間にスケジューリングすることができる。企図する所定の時間の１つは、伝送インフラストラクチャ１０７がネットワーク・トラフィックで混雑しないと思われる早朝である。既知の技法を使用するプレーヤ・アプリケーション１９５は、計画した時間にウェイクアップし、ローカル・ログ記録データベースからそのログ記録サイトに情報を伝送する。ログ記録サイト情報を検討することにより、コンテンツ・プロバイダ１０１はそのコンテンツ１１３の人気を測ることができる。
【０３７４】他の実施形態では、ログ記録サイトに後でアップロードするためにコンテンツ１１３の使用をログ記録する代わりに、コンテンツ１１３の使用中に必ずコンテンツ１１３の使用をログ記録サイトにアップロードする。たとえば、エンドユーザ装置１０９に記憶したコンテンツ１１３をＤＶＤディスク、ディジタル・テープ、フラッシュ・メモリ、ミニディスク、またはそれと同等の読取り／書込み可能取外し可能媒体などの外部装置上に複製またはコピーする場合、その使用はログ記録サイトにアップロードされる。これは、コンテンツ１１３を購入したときに伝送される使用条件２０６において、コンテンツ１１３をコピーするための前提条件になる可能性がある。これは、コンテンツ・プロバイダ１０１がコンテンツ１１３に対して自分が再生、複製、その他のアクションを行っている最中に自分のコンテンツ１１３の使用を正確に追跡できることを保証するものである。
【０３７５】そのうえ、コンテンツ１１３に関するその他の情報をログ記録サイトにアップロードすることができる。たとえば、コンテンツ１１３を最後に実行した時間（たとえば、時間および日付）、コンテンツ１１３を何回実行したか、ＤＶＤディスク、ディジタル・テープ、ミニディスクなどの許可された外部装置にコンテンツ１１３を複製またはコピーした場合などである。エンドユーザ装置１０９上の単一プレーヤ・アプリケーション１９５について、１所帯内の各種家族など、複数の別個のユーザが存在する場合、コンテンツ１１３のユーザの識別名は使用情報とともにログ記録サイトに伝送される。ログ記録サイトにアップロードされた使用情報を検討することにより、コンテンツ・プロバイダ１０１は実際の使用、ユーザの識別名、コンテンツ１１３が実行された回数に基づいてコンテンツ１１３の人気を測ることができる。実際の使用測定により、このシステムは、テレビ用のニールセン視聴率方式または電話によるアンケート調査など、一度に限られた数のユーザのみをサンプリングし、その結果を推断の基礎とするサンプリング方法を使用するシステムに比べ、より事実主導型のものになる。本実施形態では、電子ディジタル・コンテンツ・ストア１０３またはコンテンツ・プロバイダ１０１などの指定のウェブ・サイトにログオンするユーザについて、実際の使用を測定することができる。
【０３７６】４．暗号化解除１５０５、圧縮解除１５０６、再生１５０６の各コンポーネント
これらのコンポーネントでは、コピー／再生管理コンポーネントが取得したキーを使用してデータ管理およびライブラリ・アクセスの各コンポーネントから取得したオーディオ・データをアンロックし、適切な圧縮解除を適用してそれを再生用に準備し、システム・オーディオ・サービスを使用してそれを再生する。代替実施形態では、データ管理およびライブラリ・アクセスの各コンポーネントから取得したオーディオ・データをＣＤ、ディスケット、テープ、またはミニディスクなどの取外し可能媒体にコピーすることができる。
【０３７７】５．データ管理１５０２およびライブラリ・アクセス１５０３の各コンポーネント
これらのコンポーネントは、エンドユーザのシステム上で様々な記憶装置で歌曲データを記憶して取り出すと同時に記憶した歌曲に関する情報を求める要求を処理するために使用する。
【０３７８】６．アプリケーション間通信コンポーネント１５０８
このコンポーネントは、セキュア・ディジタル・コンテンツ電子配布プレーヤと、プレーヤ・アプリケーション１９５を呼び出すことができるかまたはその機能を実行するときにプレーヤ・アプリケーション１９５が使用する必要があるその他のアプリケーション（たとえば、ブラウザ、ヘルパ・アプリケーション、またはプラグイン

など）との調整のために使用する。たとえば、ＵＲＬ制御が活動化されると、それは適切なブラウザを呼び出し、適切なページをロードするようそれに指示する。

【０３７９】７．その他の各種コンポーネント

上記のカテゴリ（たとえば、インストール）に該当しない個々のコンポーネントはここにグループ化される。

【０３８０】８．汎用プレーヤ

この項では、上記のコンポーネントとプレーヤ・アプリケーション１９５のあるバージョンとの結合について説明する。プレーヤ・アプリケーション１９５はソフトウェア・オブジェクトに基づくことによってカストマイズ用に設計されているので、これは多種多様な可能な例の１つにすぎない。

【０３８１】プレーヤ・オブジェクト・マネージャ１５０１は、他のすべてのコンポーネントをまとめて保持するソフトウェア・フレームワークである。上記の各項で述べたように、この図でプレーヤ・オブジェクト・マネージャ１５０１の下にあるブロックはどのプレーヤにも必要であるが、使用する暗号化またはスクランブルの形式、オーディオ圧縮のタイプ、コンテンツ１１３のライブラリ用のアクセス方法などに応じて専用バージョンと置き換えることができる。

【０３８２】プレーヤ・オブジェクト・マネージャ１５０１の上には変数オブジェクト１５１２があり、これはたいてい再生またはサーチ中のコンテンツ１１３に関連するメタデータから導出される。これらの変数オブジェクトは、エンドユーザ表示１５１０によりエンドユーザ装置１０９に使用可能なものになり、エンドユーザ・コントロール１５１１から入力を受け取る。すべてのオブジェクトは構成可能であり、すべてのコンテナのレイアウトはカストマイズ可能である。これらのオブジェクトは、Ｃ／Ｃ＋＋、Java、またはそれと同等のプログラミング言語で実現することができる。

【０３８３】プレーヤ・アプリケーション１９５の使用

以下の実施形態は、エンドユーザ装置１０９上で実行されるプレーヤ・アプリケーション１９５がオーディオ・プレーヤであり、コンテンツ１１３が音楽である例に関するものである。ただし、当業者であれば、他のタイプのコンテンツ１１３もプレーヤ・アプリケーション１９５によってサポートできることに留意されたい。典型的なオーディオ・マニアは複数歌曲を保持するＣＤのライブラリを持っている。これらのすべては、セキュア・ディジタル・コンテンツ電子配布システム１００内で使用可能なものである。電子ディジタル・コンテンツ・ストア１０３から購入された歌曲セットは自分のシステム上のディジタル・コンテンツ・ライブラリ１９６内に記憶される。物理的なＣＤに類似した歌曲のグループ化は再生リストとして記憶される。場合によっては、再生リストが１枚のＣＤを正確にエミュレートする（たとえば、１枚の市販のＣＤのすべてのトラックがそのＣＤのオンライン・バージョンとして電子ディジタル・コンテンツ・ストア１０３から購入され、そのＣＤのものと同等の再生リストによって定義される）。しかし、ほとんどの再生リストは、エンドユーザが自分のシステム上のディジタル・コンテンツ・ライブラリに記憶した歌曲をグループ化するために、エンドユーザによってまとめられる。しかし、以下の説明のため、再生リストという用語に言及するときは、オーダメイドの音楽ＣＤの例を使用する。

【０３８４】ＳＣプロセッサ１９２アプリケーションからの呼出しにより始動させるのではなく、エンドユーザがプレーヤ・アプリケーション１９５を明示的に開始すると、それは最後にアクセスした再生リストにプリロードされる。ディジタル・コンテンツ・ライブラリ１９６にいかなる再生リストも存在しない場合、再生リスト・エディタが自動的に開始される（ユーザが優先設定によりこの機能をオフにしていない場合に限る）。詳細については以下の再生リストを参照されたい。

【０３８５】プレーヤ・アプリケーション１９５は特定の歌曲を引数として指定して呼び出すこともでき、その場合、そのアプリケーションは直ちに歌曲再生モードに入る。任意選択で、その歌曲は、再生用に準備することができるが、処理の前にエンドユーザによるアクションを待つ可能性がある。このような状況の詳細については以下の歌曲再生を参照されたい。

【０３８６】再生リスト（エンドユーザ・インタフェース１６０３の対応画面）：エンドユーザが再生リスト機能を呼び出したときに、以下の機能が使用可能になる。

・　再生リストのオープン

・　ディジタル・コンテンツ・ライブラリを呼び出して、選択のために記憶した再生リストのリストを表示する。詳細については以下のディジタル・コンテンツ・ライブラリも参照されたい。

・　再生リストの編集

・　すでにロードされている場合は現行再生リストを提供して、再生リスト・エディタ（以下を参照）を呼び出す。そうでない場合は、エディタは始めに空の再生リストを作成する。

・　再生リストの実行

・　選択した歌曲（どの歌曲も選択されない場合は再生リストの先頭）から始めて、一度に１曲ずつ歌曲を再生する。再生リスト・エディタに設定されたオプションは再生の順序付けを左右する。しかし、再生リストのこの再生に関するオプションを指定変更するために、ここではいくつかのコントロールが用意されている。

・　歌曲の再生

・　再生リストから選択した歌曲のみ再生する。詳細については以下の歌曲再生を参照されたい。

・　再生リスト情報

・　再生リストに関する情報を表示する。

・　歌曲情報
・　再生リスト内の選択した歌曲に関する情報を表示する。
・　ウェブ・サイトの訪問
・　この再生リストに関連するウェブ・サイトをブラウザにロードする。
・　ライブラリ
・　ディジタル・コンテンツ・ライブラリ・ウィンドウをオープンする。詳細については以下のディジタル・コンテンツ・ライブラリも参照されたい。
【０３８７】再生リスト・エディタ（エンドユーザ・インタフェース１６０３の対応画面）：再生リスト・エディタを呼び出す場合、エンドユーザのオプションは以下の通りである。
・　再生リストの閲覧／ロード／削除
・　ディジタル・コンテンツ・ライブラリを呼び出して、ロードまたは削除するものを選択するために、記憶した再生リストのリストを表示する。詳細については以下のディジタル・コンテンツ・ライブラリも参照されたい。
・　再生リストの保管
・　再生リストの現行バージョンをディジタル・コンテンツ・ライブラリ１９６に保管する。
・　歌曲の削除
・　現在選択した歌曲を再生リストから削除する。
・　歌曲の追加
・　再生リストに追加する歌曲を選択するために、歌曲サーチ・モードでディジタル・コンテンツ・ライブラリを呼び出す。詳細については以下のディジタル・コンテンツ・ライブラリも参照されたい。
・　歌曲情報の設定
・　再生リスト内の選択した歌曲に関する情報を表示し、それに対する変更を可能にする。この情報は再生リスト内に記憶され、ディジタル・コンテンツ・ライブラリ１９６内に記憶した歌曲に関する情報は変更しない。以下の項目を変更することができる。
・　表示した歌曲タイトル
・　歌曲に関するエンドユーザの注
・　歌曲再生時の導入遅延
・　歌曲再生後の後続遅延
・　再生時の歌曲内の開始点
・　再生時の歌曲内の終点
・　ランダム・モード用の重み付け
・　この歌曲用のボリューム調整など
【０３８８】再生リスト属性の設定：　この再生リストの属性を表示し、それに対する変更を可能にする。以下の属性を設定することができる。
・　再生リスト・タイトル
・　再生リスト・モード（ランダム、順次など）
・　反復モード（１回再生、完了時に再始動など）
・　この再生リストに関するエンドユーザの注
ライブラリ（エンドユーザ・インタフェース１６０１の対応画面）
・　ディジタル・コンテンツ・ライブラリ・ウィンドウをオープンする。詳細については以下のディジタル・コンテンツ・ライブラリも参照されたい。
【０３８９】歌曲再生
引数として歌曲を指定してプレーヤ・アプリケーション１９５を呼び出すかまたは再生リストからまたはディジタル・コンテンツ・ライブラリ内で再生用の歌曲を選択することにより、再生用に歌曲を準備すると、エンドユーザのオプション（エンドユーザ・インタフェース１６０１の対応画面）は以下の通りである。
・　再生
・　休止
・　停止
・　後退スキップ
・　前進スキップ
・　ボリュームの調整
・　トラック位置の調整
・　歌詞の閲覧
・　クレジットの閲覧
・　ＣＤカバーの閲覧
・　アーチスト・ピクチャの閲覧
・　トラック情報の閲覧
・　その他のメタデータの閲覧
・　ウェブ・サイトの訪問
・　再生リスト
・　ライブラリなど
【０３９０】ディジタル・コンテンツ・ライブラリ
ディジタル・コンテンツ・ライブラリは、歌曲または再生リストを選択したときに暗黙のうちに呼び出される場合もあれば（上記を参照）、エンドユーザのシステム上で歌曲ライブラリの管理のためにそれ専用のウィンドウにオープンすることもできる。その場合、エンドユーザのオプションは以下の通りである。
歌曲の処理：
アーチスト、カテゴリ、レーベルなどによる全曲ソート
アーチスト、カテゴリ、レーベルなどによる歌曲の選択
現行再生リストへの選択歌曲の追加
ＣＤへの歌曲のコピー（可能である場合）
歌曲の削除
カテゴリへの歌曲の追加など
再生リストの処理：
名前別のソート
カテゴリ別のソート
キーワードによるサーチ
含まれる歌曲タイトルによるサーチ
選択した再生リストのロード
再生リストの名前変更

再生リストの削除
選択した再生リストからのＣＤの作成（可能である場合）など
【０３９１】Ｅ．同報通信送達モードのエンドユーザ装置１０９
１．マルチティア・ディジタルＴＶの実施形態
次に、同報通信送達を使用するエンドユーザ装置１０９の代替実施形態について説明する。図２３に移行すると、同報通信インフラストラクチャによりコンテンツ１１３を受信するための代替実施形態が示されている。同報通信センタ１８０２により伝送されるパッケージ２００６は、セットトップ・ボックス１８０４で送受信される。セットトップ・ボックス１８０４は、以下の図２６ないし図３１に示すユーザ画面の例示的な図など、ＧＵＩ（グラフィカル・ユーザ・インタフェース）ジェネレータを使用してＧＵＩを生成する。この実施形態のＧＵＩは、ユーザが閲覧している１次プログラムによる干渉を最小限にするように、透明オーバレイを生成する。ユーザが選択を行うと、パケット・フィルタ１９０６によってパッケージが抽出される。セットトップ・ボックス１８０４は、カタログ情報を収集し、ユーザ・テレビ１８０６上にビデオ・クリップを表示し、ユーザがパッケージを選択してダウンロードできるようにするアプリケーションを実行する。セットトップ・ボックス１８０４は、所望のパッケージに関連するセクションを抽出して収集し、そのパッケージを再アセンブルする。エンドユーザ装置１０９により、ユーザはディジタル・コンテンツを記憶し再生することができる（この場合も「再生」という用語は広い意味で使用する）。セットトップ・ボックス１８０４は単一の論理モジュールであり、別々のソフトウェア・モジュールで実現することができ、そのモジュールは別々の物理装置上で実行される場合もあれば実行されない場合もある。
【０３９２】バグ・カタログで伝達される情報に基づいて、セットトップ・ボックス１８０４は、あらゆる瞬間にユーザが実行可能なアクションを表すアイコンにより部分的にビデオ・クリップにオーバレイする。ユーザが実行可能な２つの主なアクションは、現在宣伝しているコンテンツをダウンロードするよう要求することと、静的オファリングまたは動的オファリング・カタログをブラウズすることである。セットトップ・ボックス１８０４は、許されるユーザ・アクションのみの正しいアイコンにより閲覧素材にオーバレイする。
【０３９３】ユーザがダウンロードすべきコンテンツを選択した後、セットトップ・ボックス１８０４は、必要であれば、典型的なユーザ認証／クレジット許可ステップを実行するようサーバに連絡することができる。選択したパッケージが動的オファリング・セットに属す場合、セットトップ・ボックス１８０４は同報通信センタ１８０２（ただし、このようなチャネルが使用可能である場合）に連絡し、選択したパッケージの同報通信を要求する。セットトップ・ボックス１８０４の要求を受信した後、同報通信センタ１８０２はその要求を妥当性検査し、所望のパッケージの伝送をスケジューリングする。同報通信センタ１８０２は、同報通信の肯定応答ならびに選択したパッケージを伝達するカルーセルに関連する同報通信間隔によりセットトップ・ボックス１８０４に応答する。セットトップ・ボックス１８０４は、ユーザに対して同報通信間隔を表示し、特定の間隔の選択を要求することができる。
【０３９４】計画したダウンロード時間になると、セットトップ・ボックス１８０４は、バグ・カタログに指定されたディジタル・チャネルにチューニングし、多重化した同報通信ストリームから所望のパッケージ・セクションのフィルタリングを開始する。セットトップ・ボックス１８０４は、伝送エラーを検出し、破壊されたブロックを抑制する（このメカニズムはたとえば巡回冗長検査にすることができるだろう）。セットトップ・ボックス１８０４は、マスタ・カタログに含まれるパッケージ記述子情報を使用してそのパッケージを再アセンブルする。動的オファリング・セット内のパッケージのダウンロード成功後、セットトップ・ボックス１８０４は同報通信センタ１８０２に通知する。
【０３９５】また、このシステムは、同報通信センタ１８０２とセットトップ・ボックス１８０４との間の個別のユニキャスト・ネットワーク接続を使用して破壊されたセクションの回復を促進する能力も有する。通常、破壊されたセクションの数は少ないので、再伝送されるデータのボリュームは少なく、このため、カルーセル・サイクル全体を待つのとは対照的に、ユニキャストまたはマルチキャストを使用してユニキャスト・ネットワーク接続によりこれらのセクションを再伝送する方が高速になる。さらに、このチャネルによりパッケージ全体をダウンロードする方が高速になるだろうとセットトップ・ボックス１８０４が判断した場合、そのようにすることもできる。
【０３９６】パケット・フィルタ１９０６は、設定周波数またはチャネルあるいはその他の既知のフィルタリング手段に基づいてパケットをフィルタリングすることができる。カルーセルは、同報通信情報とコンテンツＳＣ６４０を受け取る。受信機は、同報通信されたパケットをコンテンツＳＣ６４０、アートワークＳＣ２０４１、グローバルＳＣ２０４０用の完全なパッケージ２００６に再アセンブルするが、これらのＳＣはまとめて同報通信ＳＣという。エンドユーザ装置１０９上で実行されるソフトウェア・アプリケーション１９１０はセットトップ・ボックス１８０４からパッケージ２００６を受け取った。この実施形態のソフトウェア・アプリケーション１９１０は、プレーヤ・アプリケーション１９１とのインタフェースを取るためにコンテンツ・ホスト・エミュ

レータ１９１２を開始するデーモンである。コンテンツ・ホスト・エミュレータ１９１２により、この同報通信インフラストラクチャと、通信インフラストラクチャ（インターネットなど）と、コンピュータ可読媒体で同じプレーヤ・アプリケーション１９１を使用することができる。プレーヤ・アプリケーション１９１と、セキュア・コンテナ・プロセッサ１９１、ヘルパ・アプリケーション１９３、ウォータマーク１９３、暗号化解除再暗号化１９４を含む関連パーツは変更されない。このため、開発者には、この同報通信実施形態と通信実施形態またはコンピュータ可読媒体実施形態用のプレーヤを構築するための１組のＡＰＩおよびツールが提供される。そのうえ、クリアリングハウス・エミュレータ１９１４により、ユーザが最終会計調停のためにエンドユーザ装置１０９を元通りクリアリング・ハウス１０５に接続するまで、トランザクションをログ記録することができる。

【０３９７】次に図２５に移行すると、本発明により図２２の代替実施形態によってコンテンツを購入するためにエンドユーザ装置上で実行されるプロセスの流れ図２１００が示されている。この流れ図をよりよく理解するために、図２６ないし図３１を参照することになるが、これは本発明による図２２の代替実施形態を使用してテレビ１８０６上で行うユーザの購入を示す一連の画面ショットである。

【０３９８】プロセス・フロー２１００はステップ２１０１から始まり、「購入」および「カタログ」アイコンが表示される。ステップ２１０４でユーザ入力を受け取る。ステップ２１０６および２１０８では、プログラム２２０４の同報通信中に「購入」または「カタログ」のユーザ選択を判定するためのテストを行う。「購入」を選択した場合、ステップ２１１０で請求のために自分自身を識別するようユーザに要求する。ステップ２１１０～２１１６および図２８に示す実施形態では、「スマート・カード」と関連の個人識別番号（ＰＩＮ）を使用する。デビット・カードの使用を含む、その他の請求メカニズムも可能である。ユーザが自分自身を識別すると、ステップ２１１８でダウンロードが開始する。ステップ２１０６で「カタログ」を選択した場合、ステップ２１２０で購入可能な製品のメニュー・パネルを表示し、ユーザは選択カーソルによりその製品間をナビゲートすることができる（ステップは図示せず）。ステップ２１２２でユーザ入力を受け取る。この入力が「購入」である場合、ビューアは認証プロセス２１１０～２１１６を続行する。入力が「終了」である場合、ビューアはステップ２１２６で「購入」および「カタログ」の選択に戻る。認証が成功すると、図３０に示すように、ダウンロード・プロセスは任意選択のメッセージがビューアに対してこれを示すことから始まる。ただし、消費者の購入活動によって中断されないビデオの上にすべてのグラフィック・イメージがオーバレイされることに留意されたい。

【０３９９】当業者であれば、本発明の同報通信実施形態により以下のものが可能になることに留意されたい。

・　ディジタル・テレビ放送インフラストラクチャによるディジタル・コンテンツの高速かつ確実なダウンロード（ディジタル・コンテンツが後で再生するためのユニットとしてダウンロードすべきパッケージである場合、どのような形式の摂取および解釈も示すように「再生」は広い意味で使用する）

・　ディジタル・テレビ放送インフラストラクチャによるディジタル・コンテンツの独立した記述。このシステムにより、コンテンツ受信側からコンテンツ送信側への戻りチャネルが使用不能である（または、滅多に使用可能にならない）ときに、ディジタル・テレビ放送インフラストラクチャによるディジタル・コンテンツのダウンロードが可能になる。

・　コンテンツ受信側からコンテンツ送信側への戻りチャネルが使用可能であるときに、ダウンロード時間の改善

・　ディジタル・テレビ放送インフラストラクチャに接続されたディジタル・セットトップ・ボックス１８０４とＴＶを使用して、ユーザがディジタル・コンテンツを選択しダウンロードすること

・　同時にビデオ・プログラムを見ながら、ユーザがディジタル・コンテンツを選択しダウンロードすること

・　グラフィックおよびビデオを使用して、コンテンツ・プロバイダがダウンロード用に使用可能なディジタル・コンテンツをプロモーションすること

・　マネージャがダウンロード用に使用可能なディジタル・コンテンツの数およびタイプをリアルタイムで更新すること

【０４００】２．個別チャネルによるウェブ同報通信の実施形態

次に、本発明の同報通信送達によりウェブ同報通信サービス内の個別チャネルを使用するエンドユーザ装置１０９の代替実施形態について説明する。図３１に移行すると、ウェブ同報通信インフラストラクチャ内の個別チャネルを使用してコンテンツ１１３を受信する代替実施形態が示されている。図３２は、本発明により図３１の代替実施形態によってコンテンツを購入するためにエンドユーザ装置上で実行されるプロセスの流れ図２８００である。セットトップ・ボックス１８０４は、以下の図３３ないし図４２に示すユーザ画面の例示的な図など、ウェブ・ストア２３０６が構築したウェブ・ページを受け取る。

【０４０１】図３３ないし図４２の例示的なユーザ画面に関連して図３２の流れ図２８００を使用する説明を以下に示す。このプロセスは、ステップ２８０２でウェブ・キャスト・チャネルによりプロモ・キャッシュ２３２

２にプロモーション素材をダウンロードすることから始まる。ユーザが「アルバム・リスト」と表示されたボタンを選択した場合、ステップ２８０６で図３３に示すような選択リストが提示される。この例では、「Madonna」、「Fleetwood Mac」、「Jewel」という３つの選択肢が可能である。これより多くの選択肢またはこれより少ない選択肢を表示することができるが、ここでは一例を示しているだけである。ユーザが「Madonna」などを選択した場合、ステップ２８１０では、図３４に示すようにそのアーチストに関する詳細が提示される。ただし、「サンプル」ボタンによって音楽のサンプルをプリビューできることに留意されたい。ユーザが「サンプル」ボタンを選択すると、ウェブ・ブラウザ１９１によるかあるいはプレーヤ・アプリケーション１９１により、プロモーション・クリップが再生される。ユーザが選択肢の購入を選択した場合、ステップ２８１２および２８１４では、図３５に示すように「口座」および「パスワード」を検証するための画面が提示される。この例では、コンテンツ１１３のプロバイダが決定するように、会計情報をウェブ・ストア２３０６と同期させるかまたはクリアリング・ハウス１０５と同期させることができる。キャッシュ・マネージャ２３２０はアルバム＋ＤＳＣバッファ２３２４を検査して、対応するコンテンツＳＣ６３０がローカルで検索用に使用可能であるかどうかを判定する。正しいコンテンツＳＣが使用可能である場合、それは取り出され、選択を処理するためにプレーヤ・アプリケーション１９５に渡される。対応するコンテンツＳＣ６３０が使用不能である場合、キャッシュ・マネージャ２３２０は次のコンテンツＳＣ６３０の同報通信に加入する。音楽の例に戻ると、同報通信およびダウンロードは「Madonna Material Girl」という選択肢である。図３６に示すようにキャッシュ・マネージャ２３２０が正しいダウンロード・チャネルおよび時間をスケジューリングすると、追加の任意選択情報を含む画面がユーザに提示される。

【０４０２】ユーザが「自分の選択」を選択した場合、図３７とステップ２８１６および２８１８に示すように、キャッシュ・マネージャ２３２０がウェブ同報通信によりダウンロードするようスケジューリングした選択肢のリストが示される。この例では、ユーザはコンテンツ１１３の第２のピースを購入するプロセスを繰り返す。コンテンツ１１３の第２のピースは「Fleetwood Mac Greatest Hits」である。次にユーザには、前述のようにステップ２８０４、２８０６、２８０８、２８１０、２８１４のプロセス・フローに対応する図３８ないし図４０が提示される。この時点ですでにユーザによって２つの選択肢が選択されているが、「自分の選択」ボタンが選択されると、ユーザには図４１の「Madonna」および「Fleetwood Mac」という２つの項目の状況が提示されるが、各選択ごとに１つずつ、２通りの状況が示されることに留意されたい。「Fleetwood Mac」に関する状況は「送達予定」である。「Madonna」に関する状況は「送達済み」であり、「ライブラリに追加」ボタンが示される。ユーザが「ライブラリに追加」ボタンと、対応するコンテンツＳＣ６３１と、ユーザが「切断」であるとき、すなわち、同報通信センタ２３０２から同報通信を受信しないときにこのプロセスを行えることを強調するためにここで呼び出されたＤＳＣとを選択すると、ステップ２８２２、２８２４、２８２６で、トリガ・マネージャ２３２６アプリケーションが始動し、アルバム＋ＤＳＣバッファ２３２４からその選択肢用のコンテンツＳＣ６３１を取り出し、それを処理のためにプレーヤ・アプリケーション１９５に送る。コンテンツＳＣ６３１を受け取ると、プレーヤ・アプリケーション１９５は「接続」実施形態に関して前述したようにコンテンツ１１３を使用する。一実施形態のプレーヤ・アプリケーション１９５は、インターネットなどのバック・チャネルを使用して、会計情報についてクリアリング・ハウス１０５と調停する。図４２は、「Madonna」というタイトルがエンドユーザ装置１０９上のライブラリ１９６に追加される例である。ライセンスＳＣ１４７は、インターネットまたはその他の通信ネットワークや同報通信を含むか、または物理的メーラを介し、ディスケット、ＤＶＤ、スマート・カード、デビット・カード、またはＣＤなどの任意のコンピュータ可読媒体を使用するエンドユーザ装置１０９に伝送することができる。このプロセス・フロー２８００はステップ２８３０で終了する。

【０４０３】個別同報通信チャネル実施形態によるこのウェブ同報通信では、オファーＳＣ６４１などのプロモーション素材を注文しブラウズするためにユーザを接続する必要がないことに留意されたい。むしろ、プロモーション素材はユーザが「切断」またはオフラインで閲覧するためにエンドユーザ装置１０９上にローカルに記憶される。

【０４０４】本発明の特定の実施形態を開示してきたが、当業者であれば、本発明の精神および範囲から逸脱せずにこの特定の実施形態に変更を加えることができることに留意されたい。したがって、本発明の範囲はこの特定の実施形態に限定されず、特許請求の範囲が本発明の範囲内のこのような応用例、修正形態、および実施形態をすべて含むことを意図するものである。

【０４０５】著作権の部分放棄

の著作権を留保する。

【０４０６】関連出願の相互参照

本出願は、「Multi-Tier Digital TV Programming for Content Distribution」について１９９９年１２月９日に出願され、本出願人に譲渡された非暫定的特許出願第　／　　号の一部継続出願である。前述の特許出願は参照によりその全体が本明細書に組み込まれる。

【０４０７】まとめとして、本発明の構成に関して以下の事項を開示する。

【０４０８】（１）複数のチャネルを備えたウェブ同報通信インフラストラクチャによりユーザのシステムに確実にデータを提供する方法であって、第１の暗号化キーを使用してデータを暗号化するステップと、第２の暗号化キーを使用して第１の暗号化解除キーを暗号化するステップと、少なくともユーザのシステム上で受信するために第１のウェブ同報通信チャネル上で暗号化データの少なくとも一部に関連するプロモーション・メタデータを同報通信するステップと、第２の同報通信チャネルにより暗号化データの少なくとも一部を同報通信するステップと、暗号化した第１の暗号化解除キーをコンピュータ可読媒体によりユーザのシステムに転送するステップであって、その暗号化した第１の暗号化解除キーが第２の暗号化キーによって暗号化されているステップとを含む方法。

（２）プロモーション・メタデータを同報通信するステップが、所定の時間間隔で定期的にプロモーション・メタデータを同報通信することを含む、上記（１）に記載の方法。

（３）プロモーション・メタデータを同報通信するステップが、少なくともプロモーション・メタデータをウェブ・ブラウザにより読取り可能なフォーマットに変換するサブステップを含む、上記（１）に記載の方法。

（４）暗号化データの少なくとも一部を同報通信するステップが、暗号化データの少なくとも一部に関する同報通信時間およびウェブ同報通信チャネルのスケジュールを同報通信することを含む、上記（１）に記載の方法。

（５）第２のウェブ同報通信チャネルにより暗号化データの少なくとも一部を同報通信するステップが、DirecPCTMと互換性のあるフォーマットで暗号化データを同報通信することを含む、上記（１）に記載の方法。

（６）プロモーション・メタデータがそのデータに関する同報通信時間のスケジュールを含む、上記（１）に記載の方法。

（７）複数のチャネルによりウェブ同報通信インフラストラクチャからユーザのシステム上で確実にデータを受信する方法であって、第１のウェブ同報通信チャネルからプロモーション・メタデータを受信するステップであって、そのプロモーション・メタデータが受信用に使用可能なデータに関するメタ・データであるステップと、プロモーション・メタデータの少なくとも一部をユーザによる検討用のプロモーション・オファリングにアセンブルするステップと、プロモーション・メタデータに関連して受信すべきデータをユーザによって選択するステップと、第２のウェブ同報通信チャネルからデータを受信するステップであって、そのデータがプロモーション・メタデータから選択されたデータであり、そのデータが第１の暗号化キーを使用してあらかじめ暗号化されているステップと、コンピュータ可読媒体により第１の暗号化解除キーを受信するステップであって、その第１の暗号化解除キーが第２のウェブ同報通信チャネルにより受信したデータの少なくとも一部を暗号化解除するキーであるステップとを含む方法。

（８）プロモーション・データの少なくとも一部をアセンブルするステップが、プロモーション・データの少なくとも一部をウェブ・ブラウザにより読取り可能なフォーマットにアセンブルすることを含み、選択するステップが、ウェブ・ブラウザにより選択することを含む、上記（７）に記載の方法。

（９）選択するステップが、ユーザのシステム上であらかじめ受信され記憶されたプロモーション素材を選択することを含む、上記（７）に記載の方法。

（１０）選択するステップが、選択したデータの次のウェブ同報通信に関するスケジュールを決定するサブステップと、ユーザのシステムを起動して第２のチャネル上で次のウェブ同報通信を受信するトリガを設定するサブステップとをさらに含む、上記（９）に記載の方法。

（１１）第２のウェブ同報通信チャネルからデータを受信するステップが、トリガによって提供されたウェブ同報通信チャネルおよび時間においてプロモーション・メタデータから選択したデータを受信することを含む、上記（１０）に記載の方法。

（１２）第２のウェブ同報通信チャネルからデータを受信するステップが、DirecPCTMと互換性のあるフォーマットでデータを受信することを含む、上記（７）に記載の方法。

（１３）第２のウェブ同報通信チャネルからデータを受信するステップが、ユーザのシステムが選択したデータを受信することを許可されていることをバック・チャネルにより認可するサブステップを含み、第１の暗号化解除キーを受信するステップが、ユーザのシステムが選択したデータを受信することを許可されている場合にのみ第１の暗号化解除キーを受信することを含む、上記（７）に記載の方法。

（１４）第２のウェブ同報通信チャネルからデータを受信するステップが、プロモーション・メタデータから選択したデータがユーザのシステム上で受信された場合に、次にユーザがユーザのシステムを始動するときにユーザに状況を通知するサブステップをさらに含む、上記（７）に記載の方法。

（１５）第１の暗号化解除キーを受信するステップが、第２の暗号化キーにより暗号化された第１の暗号化解除キーを受信することを含む、上記（７）に記載の方法。
（１６）第１の暗号化解除キーを受信するステップが、同報通信ストリームにより第１の暗号化解除キーを受信することを含む、上記（１５）に記載の方法。
（１７）第２の暗号化解除キーがクリアリングハウスからユーザのシステムに送信される、上記（１５）に記載の方法。
（１８）第２の暗号化解除キーが、クリアリングハウスからユーザのシステムに送信された第２の暗号化キーにより暗号化されたデータを暗号化解除するタイムアウト設備を有する、上記（１５）に記載の方法。
（１９）複数のチャネルを備えたウェブ同報通信インフラストラクチャによりユーザのシステムに確実にデータを提供するシステムであって、コンテンツ・システムと、第１の公開キーと、第１の公開キーに対応する第１の秘密キーと、データ暗号化キーと、データ暗号化キーを使用して暗号化したデータを暗号化解除するデータ暗号化解除キーと、データ暗号化解除キーのみによって暗号化解除可能になるようにデータを暗号化する第１のデータ暗号化手段と、データ暗号化解除キーを暗号化するために第１の公開キーを使用する第２のデータ暗号化手段と、クリアリング・ハウスと、第２のウェブ同報通信チャネル上で同報通信されるデータに関連するプロモーション・データを第１のウェブ同報通信チャネル上の１つまたは複数のユーザのシステムに同報通信し、データ暗号化キーにより暗号化したデータを第２の同報通信チャネル上で同報通信する同報通信センタと、暗号化されたデータ暗号化解除キーをクリアリング・ハウスに転送する第１の転送手段であって、クリアリング・ハウスが第１の秘密キーを所有する第１の転送手段と、第１の秘密キーを使用してデータ暗号化解除キーを暗号化解除する第１の暗号化解除手段と、第２の公開キーと、第２の公開キーに対応する第２の秘密キーと、第２の公開キーを使用してデータ暗号化解除キーを再暗号化する再暗号化手段と、再暗号化されたデータ暗号化解除キーをユーザのシステムに転送する第２の転送手段であって、ユーザのシステムが第２の秘密キーを所有する第２の転送手段と、第２の秘密キーを使用して再暗号化したデータ暗号化解除キーを暗号化解除する第２の暗号化解除手段とを含むシステム。
（２０）プロモーション・メタデータがそのデータに関する同報通信時間のスケジュールを含む、上記（１９）に記載のシステム。
（２１）複数のチャネルによりウェブ同報通信インフラストラクチャから確実にデータを受信する、ユーザのシステムであって、第１のウェブ同報通信チャネルからプロモーション・メタデータを受信する受信機であって、そのプロモーション・メタデータが受信用に使用可能なデータに関するメタデータである受信機と、プロモーション・メタデータの少なくとも一部をユーザによる検討用に提示する出力装置へのインタフェースと、プロモーション・メタデータに関連して受信すべきデータに関するユーザによる選択を受信する入力装置へのインタフェースと、第２のウェブ同報通信チャネルからデータを受信するよう受信機を制御する制御装置であって、そのデータがプロモーション・メタデータから選択されたデータであり、そのデータが第１の暗号化キーを使用してあらかじめ暗号化されている制御装置と、コンピュータ可読媒体により第１の暗号化解除キーを受信するインタフェースであって、その第１の暗号化解除キーが第２のウェブ同報通信チャネルにより受信したデータの少なくとも一部を暗号化解除するキーであるインタフェースとを含むユーザのシステム。
（２２）出力装置がウェブ・ブラウザであり、入力装置がユーザによる選択を受信するためにウェブ・ブラウザに結合されている、上記（２１）に記載のユーザのシステム。
（２３）制御装置が、プロモーション・メタデータから導出したスケジュールであって、第２のウェブ同報通信チャネルからデータを受信するよう受信機を制御するために使用するスケジュールをさらに含む、上記（２１）に記載のユーザのシステム。
（２４）受信機が、DirecPCTMと互換性のあるフォーマットで同報通信されたデータを受信するよう適合されている、上記（２１）に記載のユーザのシステム。

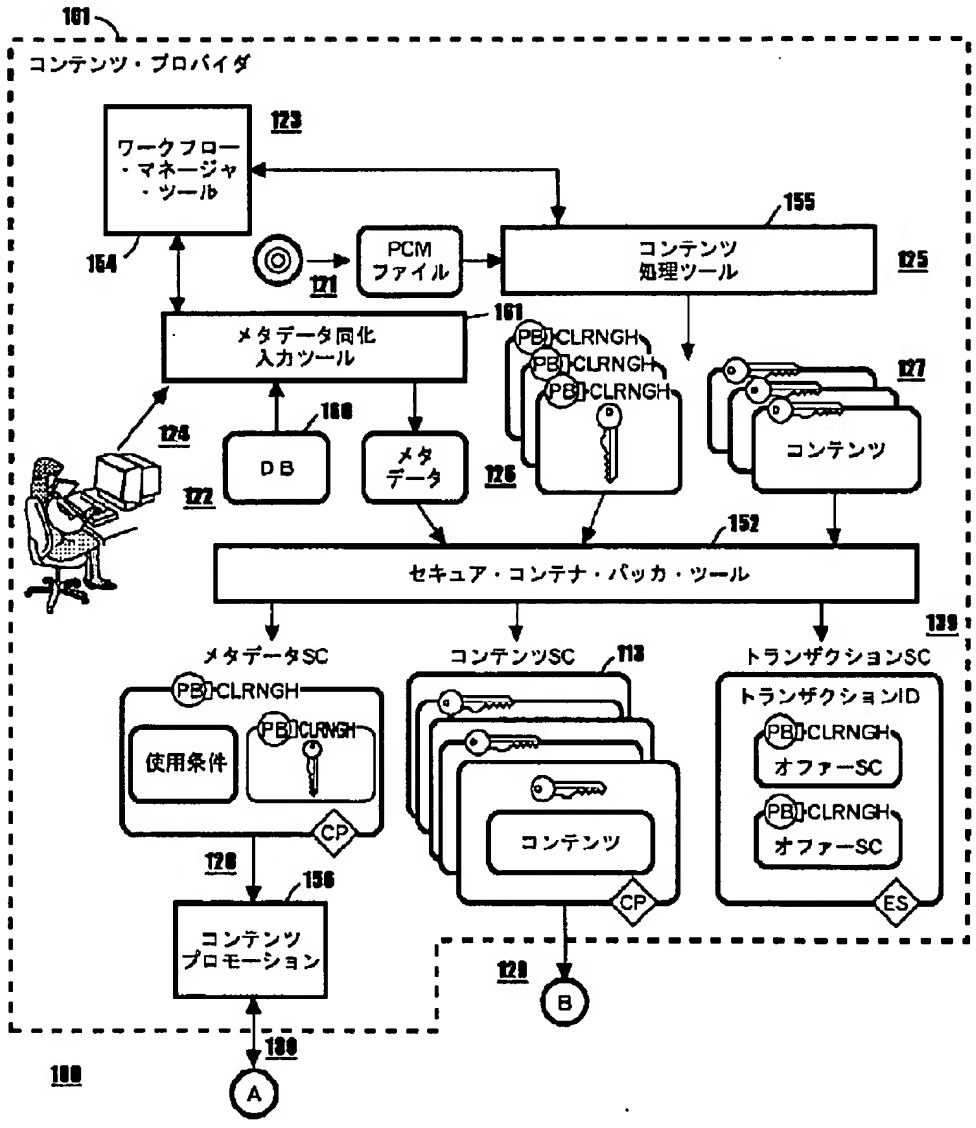
【図面の簡単な説明】
【図１】本発明によるセキュア・ディジタル・コンテンツ電子配布システムの概要を示すブロック図である。
【図２】本発明によるセキュア・ディジタル・コンテンツ電子配布システムの概要を示すブロック図である。
【図３】本発明によるセキュア・ディジタル・コンテンツ電子配布システムの概要を示すブロック図である。
【図４】本発明によるセキュア・ディジタル・コンテンツ電子配布システムの概要を示すブロック図である。
【図５】本発明によるセキュア・コンテナ（ＳＣ）の一例と関連の図形表現を示すブロック図である。
【図６】本発明によるセキュア・コンテナ（ＳＣ）用の暗号化プロセスの概要を示すブロック図である。
【図７】本発明によるセキュア・コンテナ（ＳＣ）用の暗号化解除プロセスの概要を示すブロック図である。
【図８】本発明により図１ないし図４のセキュア・ディジタル・コンテンツ電子配布システムの権利管理アーキテクチャ用の諸層の概要を示すブロック図である。
【図９】図８のライセンス制御層に適用されたときのコンテンツ配布ライセンス制御の概要を示すブロック図である。
【図１０】本発明により図１ないし図４のワーク・フロー・マネージャ・ツール用のユーザ・インタフェースの

一例を示す図である。
【図１１】本発明により図１０のユーザ・インタフェースに対応するワーク・フロー・マネージャの主要ツール、コンポーネント、プロセスを示すブロック図である。
【図１２】本発明により図１ないし図４の電子ディジタル・コンテンツ・ストアの主要ツール、コンポーネント、プロセスを示すブロック図である。
【図１３】本発明により図１ないし図４のエンドユーザ装置の主要コンポーネントおよびプロセスを示すブロック図である。
【図１４】本発明により図１１のコンテンツ前処理圧縮ツール用のコード化速度係数を計算するための方法の流れ図である。
【図１５】本発明により図１１の自動メタデータ収集ツール用の追加情報を自動的に検索するための方法の流れ図である。
【図１６】本発明により図１１の前処理圧縮ツールの前処理圧縮パラメータを自動的に設定するための方法の流れ図である。
【図１７】本発明により図１８ないし図１９に記載するようにローカル・ライブラリにコンテンツをダウンロードするプレーヤ・アプリケーションのユーザ・インタフェース画面の一例を示す図である。
【図１８】本発明により図１２のエンドユーザ装置上で実行されるプレーヤ・アプリケーションの主要コンポーネントおよびプロセスを示すブロック図である。
【図１９】本発明により図１２のエンドユーザ装置上で実行されるプレーヤ・アプリケーションの主要コンポーネントおよびプロセスを示すブロック図である。
【図２０】本発明により図１８ないし図１９のプレーヤ・アプリケーションのユーザ・インタフェース画面の一例を示す図である。
【図２１】本発明により図１１の自動メタデータ収集ツール用の追加情報を自動的に検索するための代替実施形態の流れ図である。
【図２２】本発明により同報通信インフラストラクチャを使用するディジタル・コンテンツの電子配布の代替実施形態を示す高レベル論理図である。
【図２３】図２２の詳細ブロック図であり、本発明により同報通信インフラストラクチャを使用するディジタル・コンテンツの電子配布の代替実施形態を示す図である。
【図２４】本発明により図２２の代替実施形態で同報通信されるパケットのブロック図である。
【図２５】本発明により図２２の代替実施形態によってコンテンツを購入するためにエンドユーザ装置上で実行されるプロセスの流れ図である。
【図２６】本発明により図２２の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図２７】本発明により図２２の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図２８】本発明により図２２の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図２９】本発明により図２２の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図３０】本発明により図２２の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図３１】図２２の詳細ブロック図であり、本発明によりウェブ同報通信サービス内の個別チャネルを使用するディジタル・コンテンツの電子配布の代替実施形態を示す図である。
【図３２】本発明により図３１の代替実施形態によってコンテンツを購入するためにエンドユーザ装置上で実行されるプロセスの流れ図である。
【図３３】本発明により図３１の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図３４】本発明により図３１の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図３５】本発明により図３１の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図３６】本発明により図３１の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図３７】本発明により図３１の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図３８】本発明により図３１の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図３９】本発明により図３１の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図４０】本発明により図３１の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図４１】本発明により図３１の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。
【図４２】本発明により図３１の代替実施形態を使用してテレビ上で行われるユーザの購入を示す画面ショットである。

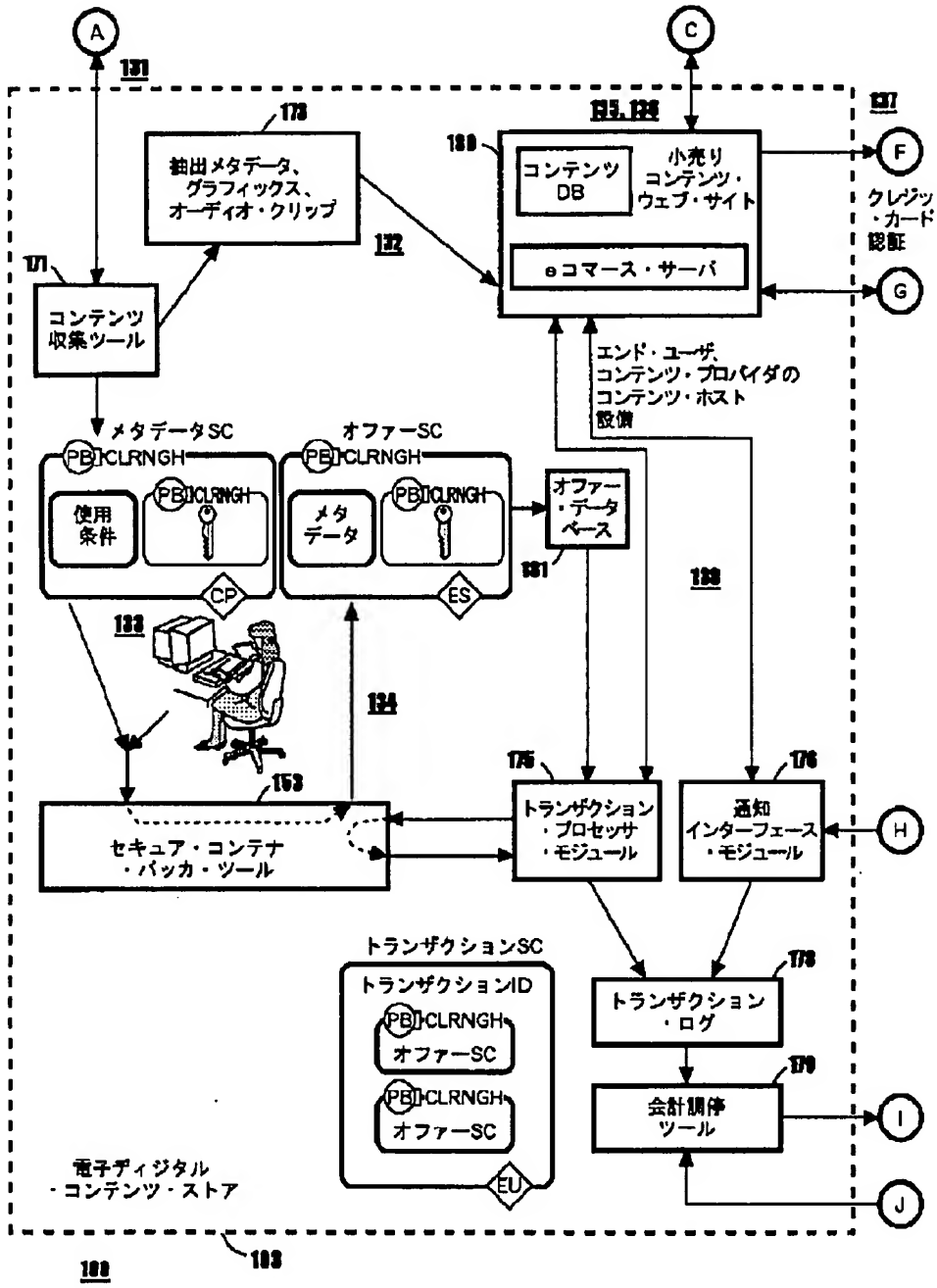
【符号の説明】

１００　セキュア・ディジタル・コンテンツ電子配布システム
１０１　コンテンツ・プロバイダ
１０３　電子ディジタル・コンテンツ・ストア
１０５　クリアリング・ハウス
１０７　伝送インフラストラクチャ
１０９　エンドユーザ装置
１１１　コンテンツ・ホスト・サイト
１１３　コンテンツ
１５２　セキュア・コンテナ・パッカ・ツール
１５４　ワーク・フロー・マネージャ・ツール
１５５　コンテンツ処理ツール
１５６　コンテンツ・プロモーション
１６０　データベース
１６１　メタデータ同化入力ツール

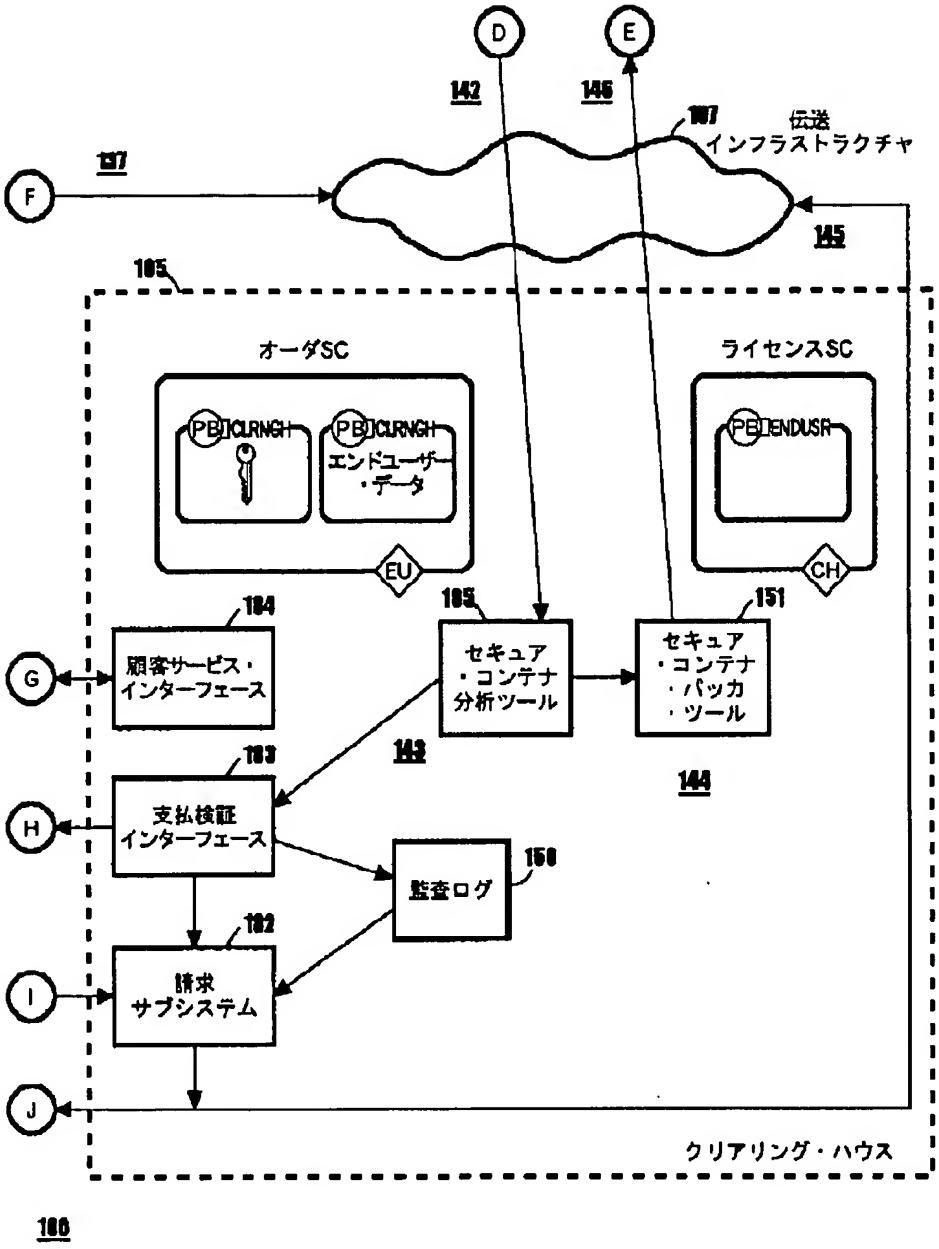
【図１】



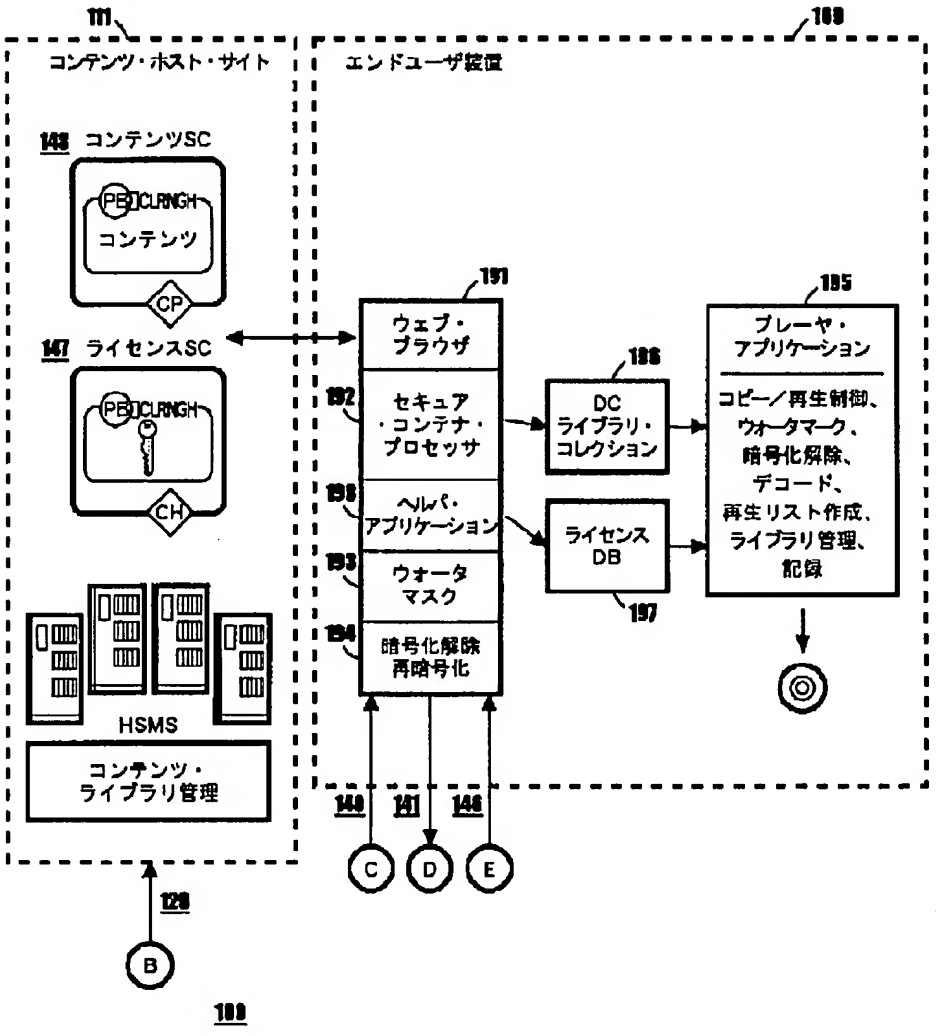
【図２】


A
C
131
137
178
抽出メタデータ、
グラフィックス、
オーディオ・クリップ
135, 136
189
コンテンツ
DB
小売り
コンテンツ・
ウェブ・サイト
F
クレジット
・カード
認証
172
eコマース・サーバ
G
171
コンテンツ
収集ツール
エンド・ユーザ、
コンテンツ・プロバイダの
コンテンツ・ホスト
設備
メタデータSC
オファーSC
PBI
CLRNGH
使用
条件
メタ
データ
CP
ES
オファー
・データ
ベース
181
180
133
134
153
175
176
トランザクション
・プロセッサ
・モジュール
通知
インターフェース
・モジュール
H
セキュア・コンテナ
・パッカ・ツール
トランザクションSC
トランザクションID
オファーSC
178
トランザクション
・ログ
179
会計調停
ツール
I
J
EU
電子ディジタル
・コンテンツ・ストア
188
183

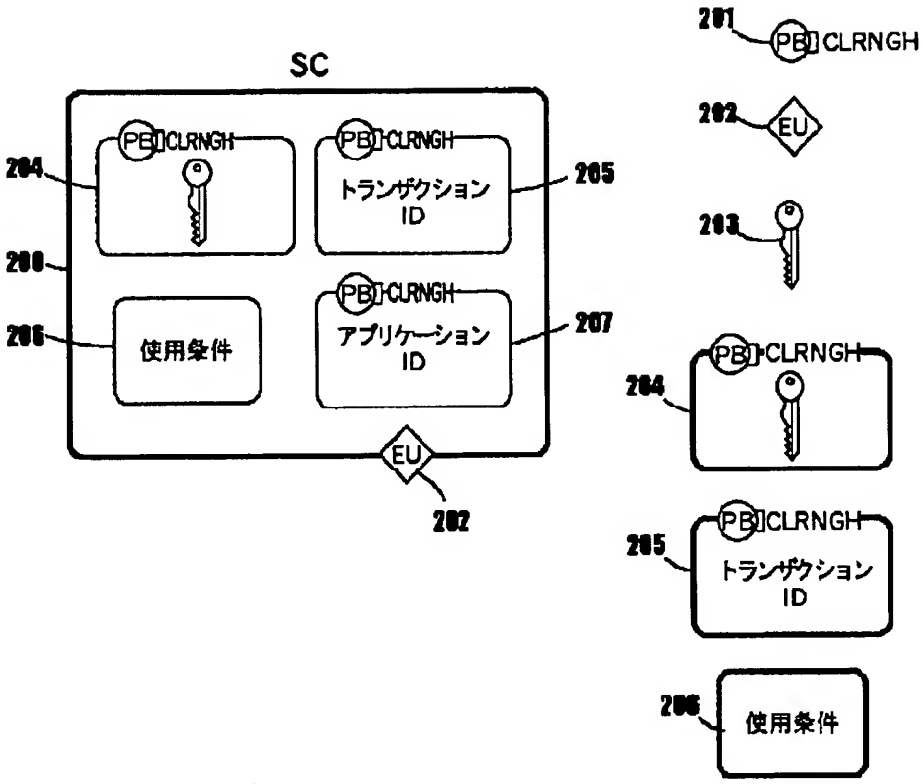
【図３】


D
E
142
146
147
伝送
インフラストラクチャ
F
145
105
オーダSC
ライセンスSC
PBJCLRNGH
PBJCLRNGH
エンドユーザー
・データ
PBJENDUSR
EU
CH
104
105
151
顧客サービス・
インターフェース
セキュア
・コンテナ
分析ツール
セキュア
・コンテナ
・パッカ
・ツール
G
143
144
103
支払検証
インターフェース
H
監査ログ
150
102
請求
サブシステム
I
J
クリアリング・ハウス
100

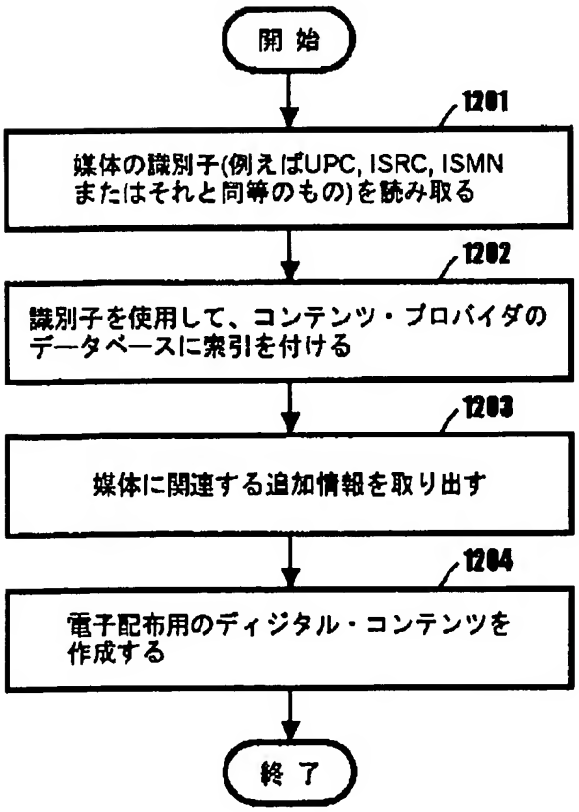
【図４】


111
コンテンツ・ホスト・サイト
エンドユーザ装置
148 コンテンツSC
PBDCLRNGH
コンテンツ
CP
147 ライセンスSC
PBDCLRNGH
CH
HSMS
コンテンツ・
ライブラリ管理
151
ウェブ・
ブラウザ
152
セキュア
・コンテナ・
プロセッサ
153
ヘルパ・
アプリケーション
153
ウォータ
マスク
154
暗号化解除
再暗号化
156
DC
ライブラリ・
コレクション
157
ライセンス
DB
155
プレーヤ・
アプリケーション
コピー／再生制御、
ウォータマーク、
暗号化解除、
デコード、
再生リスト作成、
ライブラリ管理、
記録
149
141
146
C
D
E
120
B
100

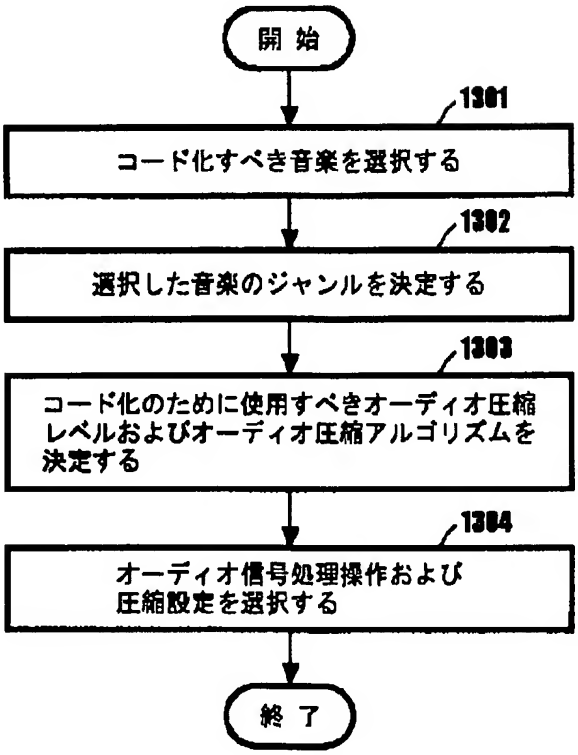
【図５】


SC
PB CLRNGH
204
PB CLRNGH
トランザクション ID
205
200
206
使用条件
PB CLRNGH
アプリケーション ID
207
EU
202
201
PB CLRNGH
202
EU
203
PB CLRNGH
204
PB CLRNGH
205
トランザクション ID
206
使用条件

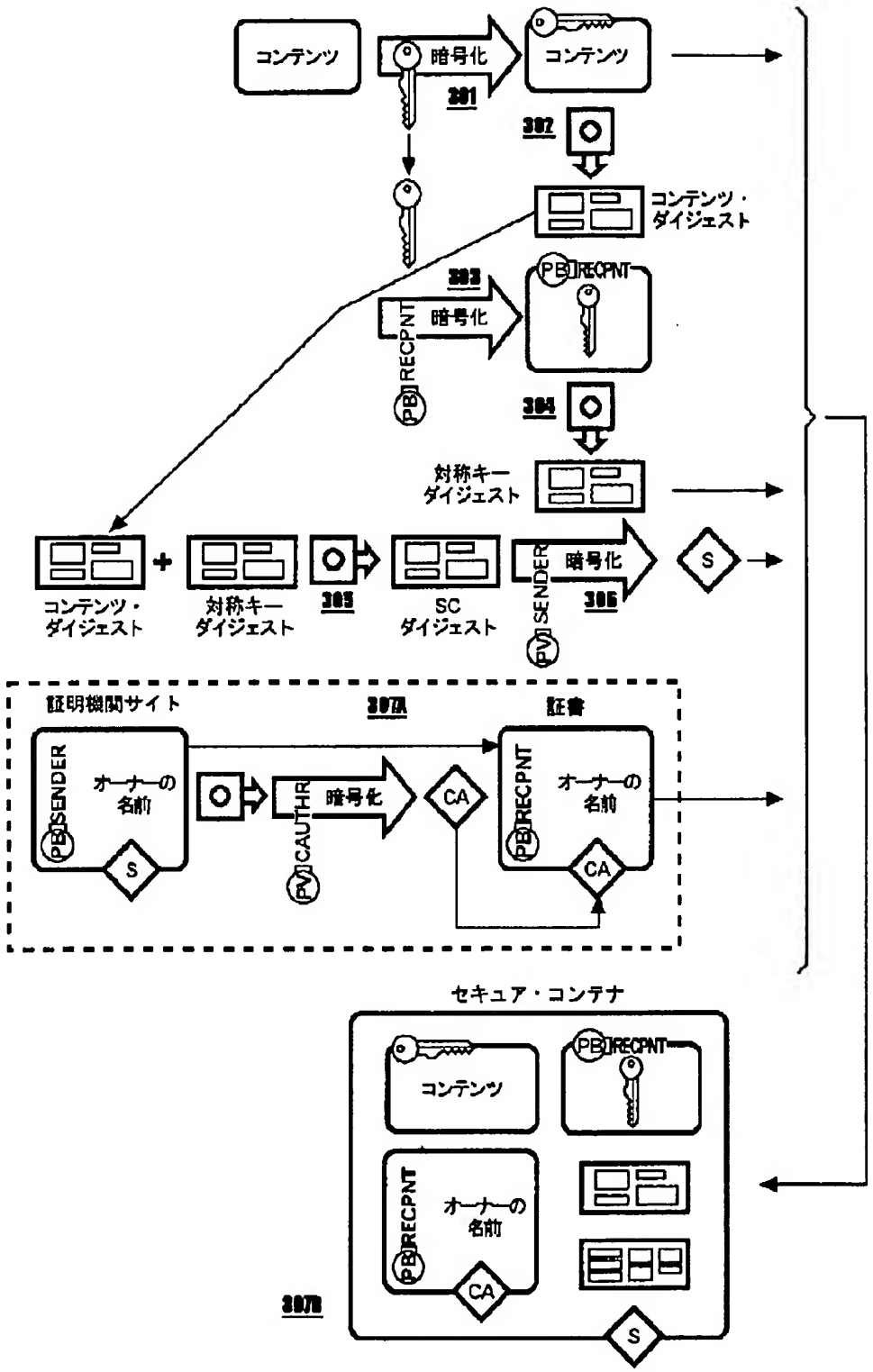
【図１５】


開 始
1201
媒体の識別子(例えばUPC, ISRC, ISMN またはそれと同等のもの)を読み取る
1202
識別子を使用して、コンテンツ・プロバイダのデータベースに索引を付ける
1203
媒体に関連する追加情報を取り出す
1204
電子配布用のディジタル・コンテンツを作成する
終 了

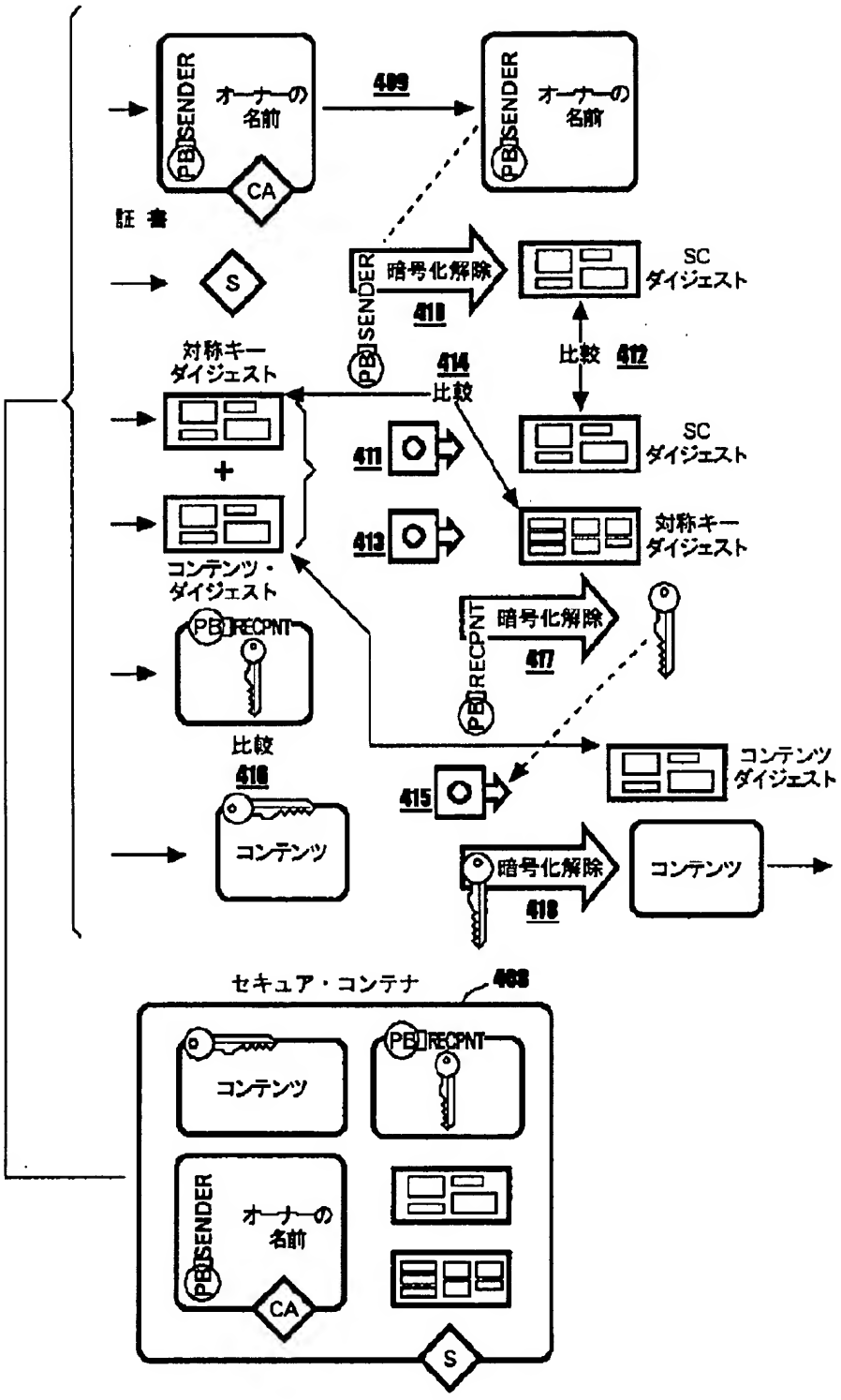
【図１６】


開 始
1301
コード化すべき音楽を選択する
1302
選択した音楽のジャンルを決定する
1303
コード化のために使用すべきオーディオ圧縮レベルおよびオーディオ圧縮アルゴリズムを決定する
1304
オーディオ信号処理操作および圧縮設定を選択する
終 了

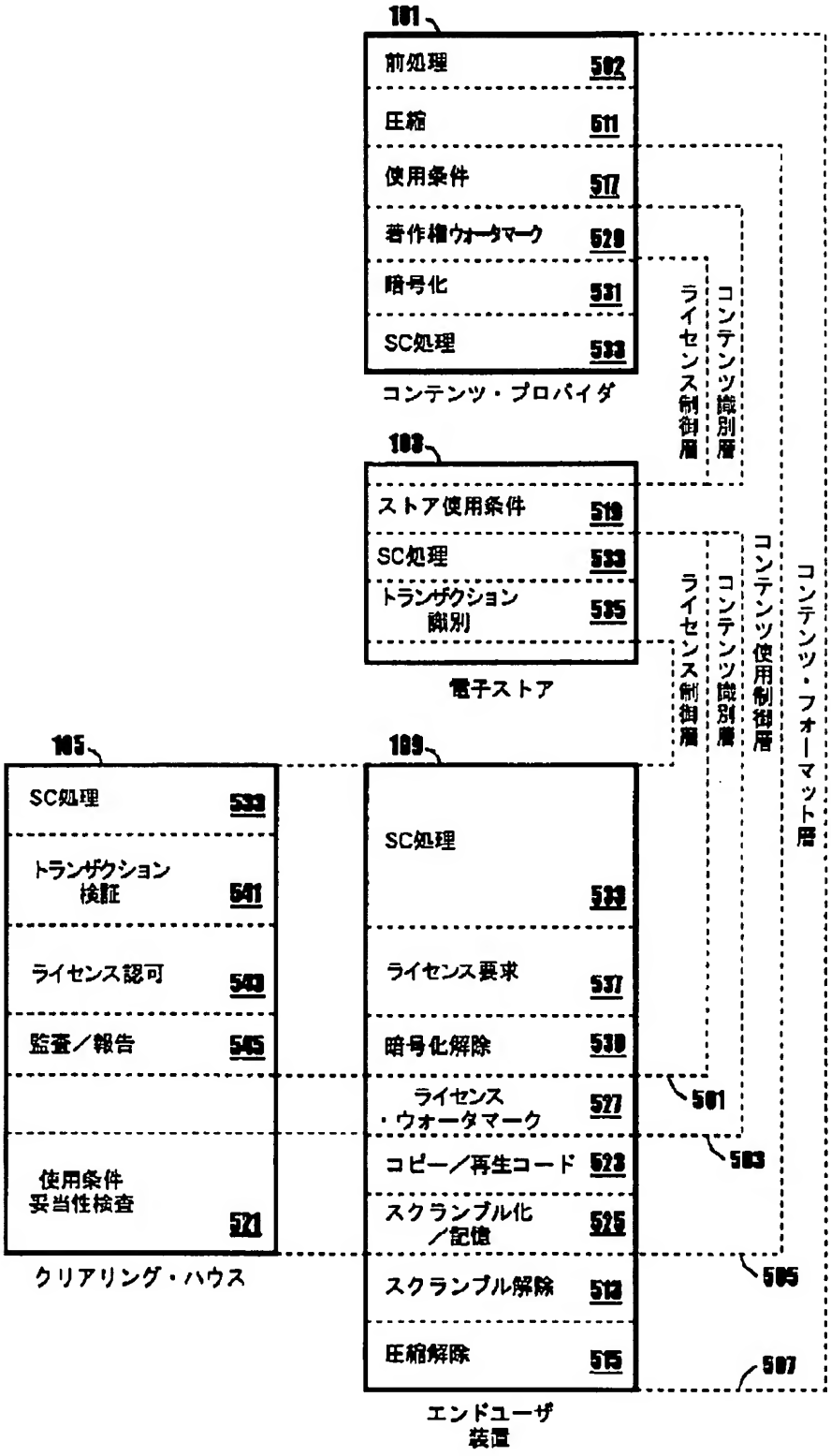
【図６】


コンテンツ
暗号化
コンテンツ
301
302
コンテンツ・
ダイジェスト
PB RECPNT
303
暗号化
PB RECPNT
304
対称キー
ダイジェスト
コンテンツ・
ダイジェスト
対称キー
ダイジェスト
305
SC
ダイジェスト
PV SENDER
暗号化
306
S
証明機関サイト
307A
証書
PB SENDER
オーナーの
名前
S
暗号化
PV CAUTHR
CA
PB RECPNT
オーナーの
名前
CA
セキュア・コンテナ
コンテンツ
PB RECPNT
PB RECPNT
オーナーの
名前
CA
S
307B

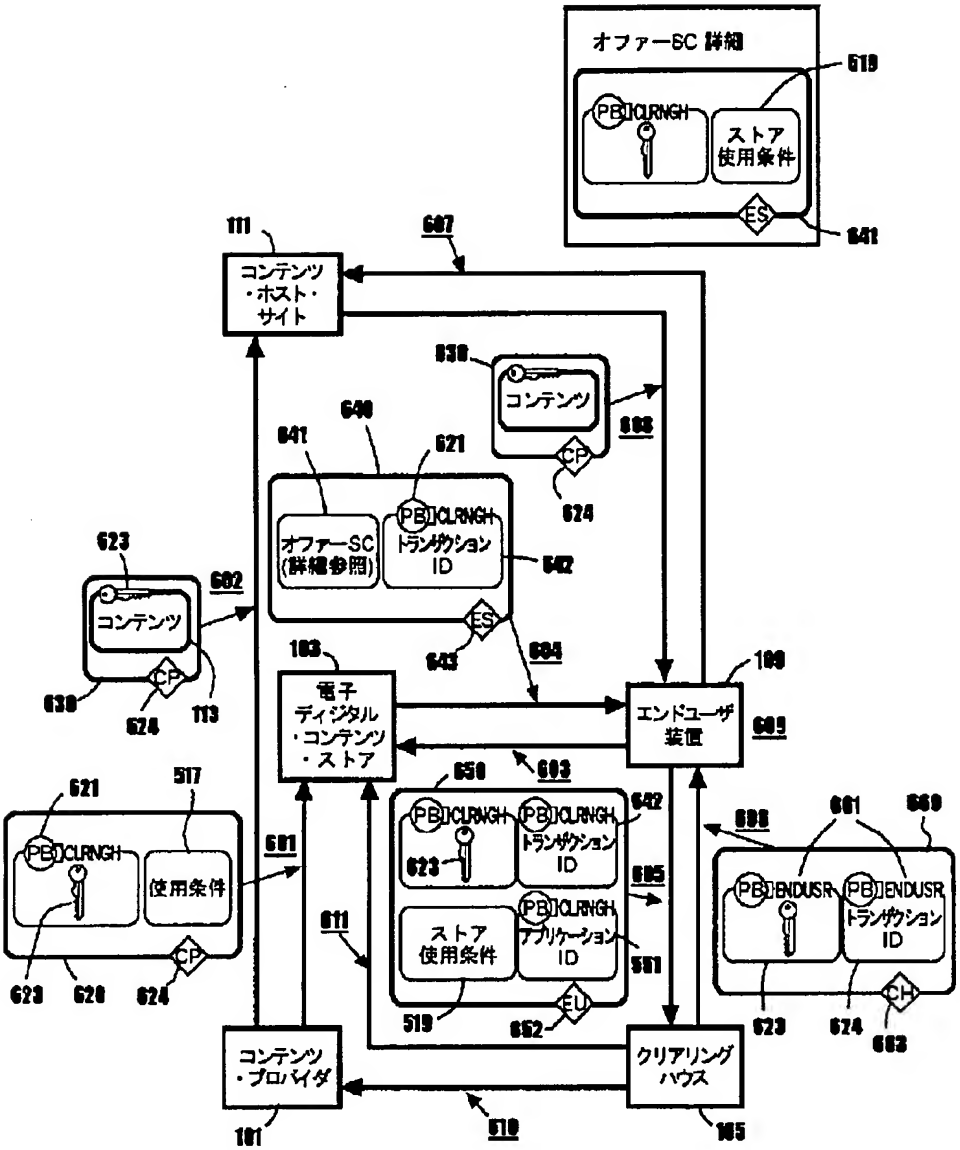
【図７】


PB SENDER
オーナーの名前
CA
409
証書
S
暗号化解除
410
SC ダイジェスト
比較 412
対称キー ダイジェスト
414 比較
411
413
コンテンツ・ダイジェスト
PB RECPNT
暗号化解除
417
比較
416
415
コンテンツ ダイジェスト
コンテンツ
暗号化解除
418
セキュア・コンテナ
403
コンテンツ
PB RECPNT
PB SENDER
オーナーの名前
CA
S

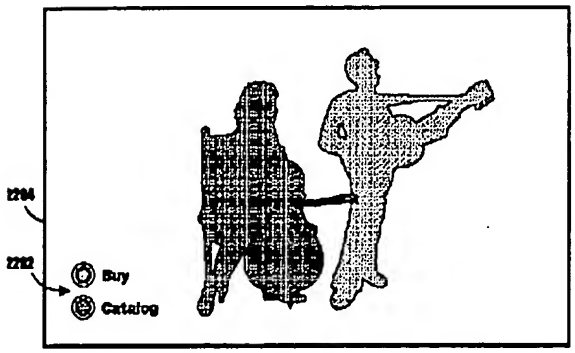
【図８】


101
前処理 502
圧縮 511
使用条件 517
著作権ウォータマーク 529
暗号化 531
SC処理 533
コンテンツ・プロバイダ
103
ストア使用条件 519
SC処理 533
トランザクション識別 535
電子ストア
105
SC処理 533
トランザクション検証 541
ライセンス認可 543
監査／報告 545
使用条件妥当性検査 521
クリアリング・ハウス
109
SC処理 533
ライセンス要求 537
暗号化解除 539
ライセンス・ウォータマーク 527
コピー／再生コード 523
スクランブル化／記憶 525
スクランブル解除 513
圧縮解除 515
エンドユーザ装置
501
503
505
507
ライセンス制御層
コンテンツ識別層
コンテンツ使用制御層
コンテンツ・フォーマット層

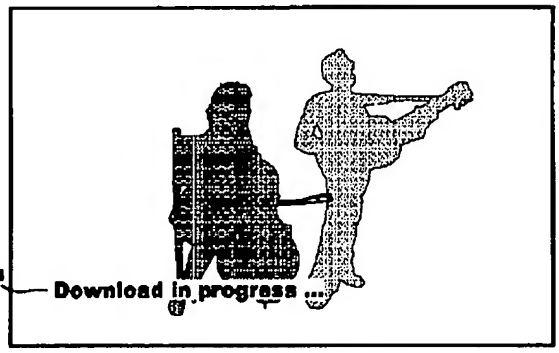
【図９】


オファーSC 詳細
619
PB CLRNGH
ストア
使用条件
ES
641
111
コンテンツ
・ホスト・
サイト
607
638
コンテンツ
CP
624
603
640
641
621
オファーSC
(詳細参照)
PB CLRNGH
トランザクション
ID
642
643
604
623
602
コンテンツ
CP
638
624
113
163
電子
ディジタル
・コンテンツ
・ストア
100
エンドユーザ
装置
609
603
650
621
517
PB CLRNGH
使用条件
CP
623
626
624
691
PB CLRNGH
PB CLRNGH
トランザクション
ID
623
642
695
611
ストア
使用条件
PB CLRNGH
アプリケーション
ID
691
519
EU
652
888
661
660
PB ENDUSR
PB ENDUSR
トランザクション
ID
CH
623
624
662
コンテンツ
・プロバイダ
101
610
クリアリング
ハウス
105

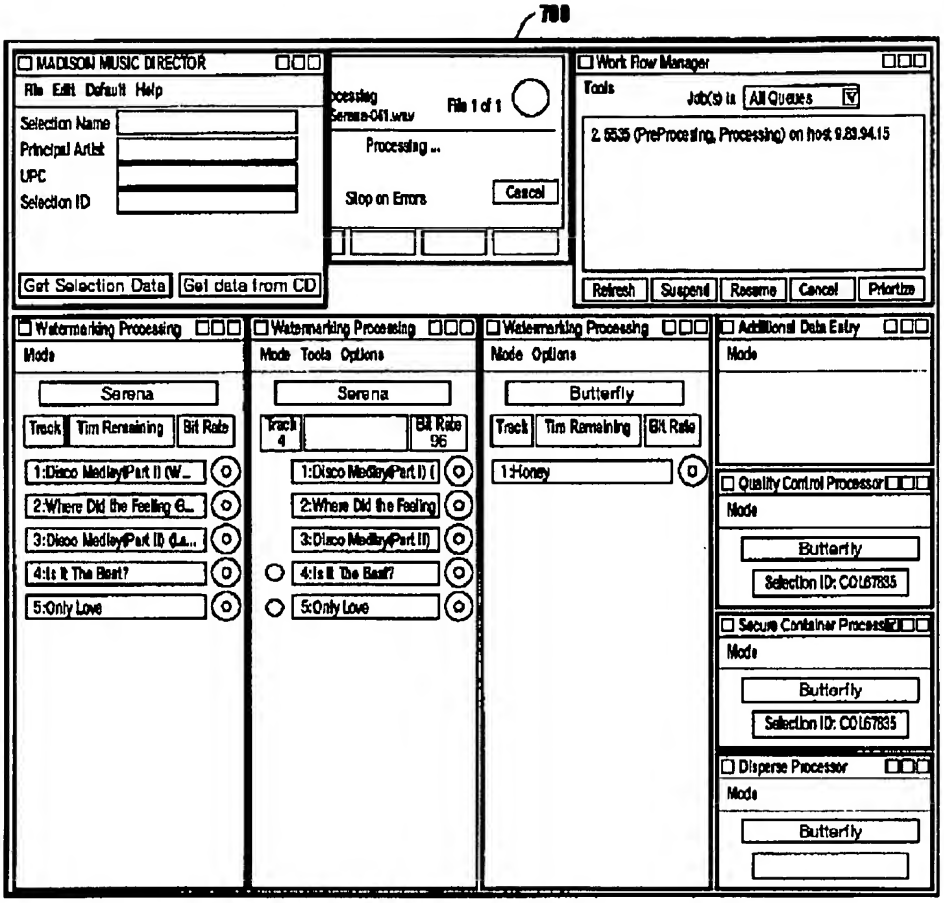
【図２６】


2204
2202
Buy
Catalog

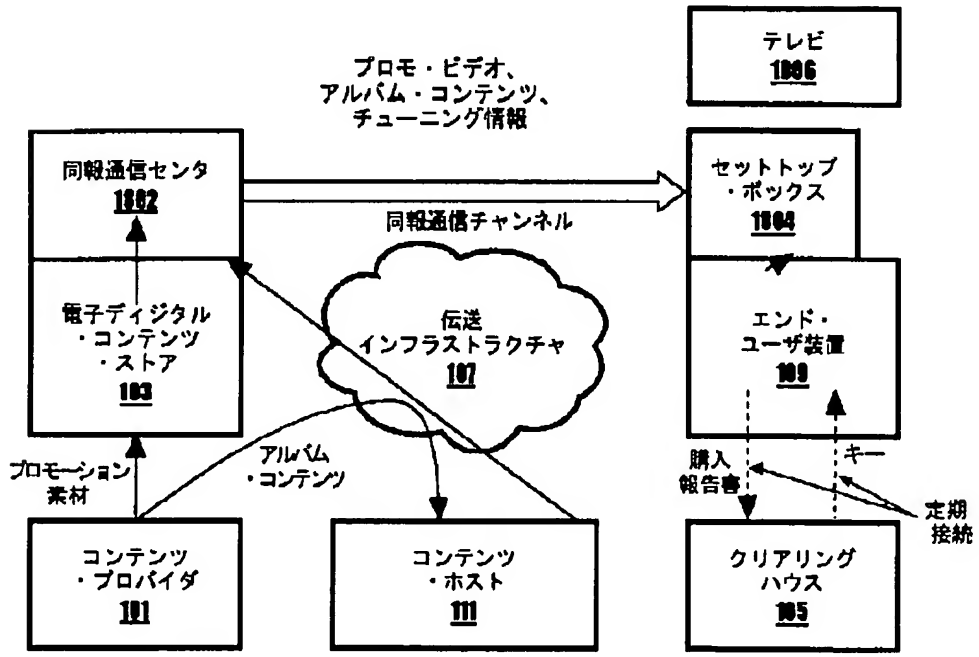
【図２８】


2804
Download in progress ...

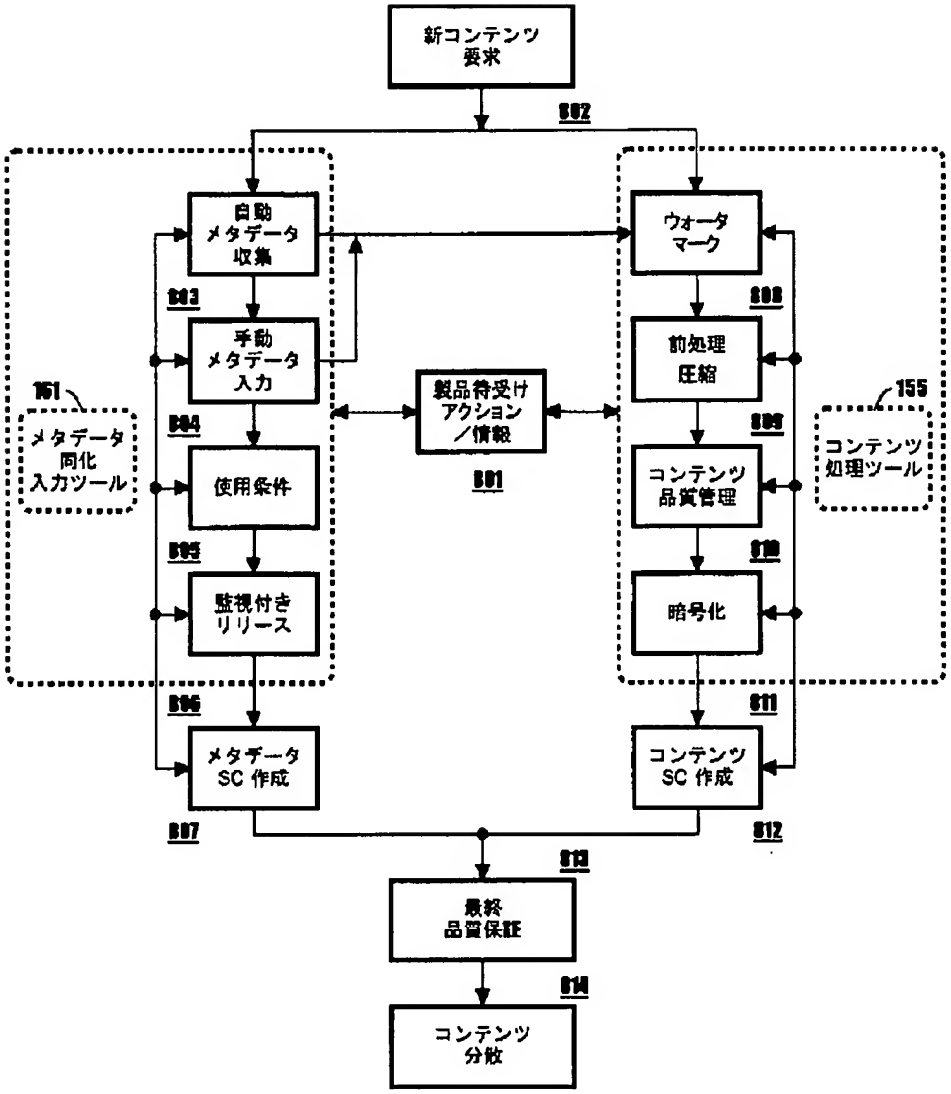
【図１０】


700
MADISON MUSIC DIRECTOR
File Edit Default Help
Selection Name
Principal Artist
UPC
Selection ID
Get Selection Data
Get data from CD
File 1 of 1
Processing ...
Stop on Errors
Cancel
Work Flow Manager
Tools
Job(s) in
All Queues
2, 6535 (PreProcessing, Processing) on host 9.83.94.15
Refresh
Suspend
Resume
Cancel
Prioritize
Watermarking Processing
Mode
Serena
Track
Tim Remaining
Bit Rate
1:Disco Medley(Part I) (W...
2:Where Did the Feeling G...
3:Disco Medley(Part II) (La...
4:Is It The Beat?
5:Only Love
Mode Tools Options
Serena
Track 4
Bit Rate 96
1:Disco Medley(Part I) (
2:Where Did the Feeling
3:Disco Medley(Part II)
4:Is It The Beat?
5:Only Love
Mode Options
Butterfly
Track
Tim Remaining
Bit Rate
1:Honey
Additional Data Entry
Mode
Quality Control Processor
Mode
Butterfly
Selection ID: C0167835
Secure Container Process
Mode
Butterfly
Selection ID: C0167835
Disperse Processor
Mode
Butterfly

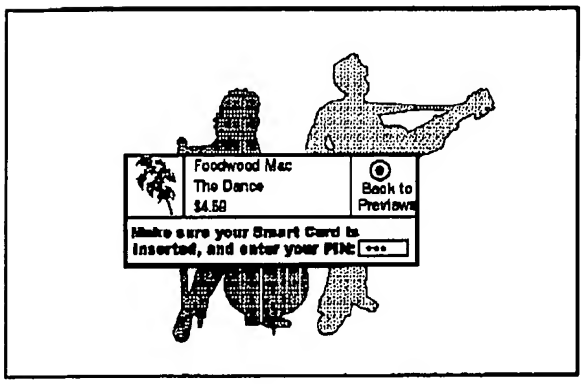
【図２２】


テレビ
1006
プロモ・ビデオ、
アルバム・コンテンツ、
チューニング情報
同報通信センタ
1002
同報通信チャンネル
セットトップ
・ボックス
1004
電子ディジタル
・コンテンツ
・ストア
103
伝送
インフラストラクチャ
107
エンド・
ユーザ装置
109
プロモーション
素材
アルバム
・コンテンツ
購入
報告書
キー
定期
接続
コンテンツ
・プロバイダ
101
コンテンツ
・ホスト
111
クリアリング
ハウス
105

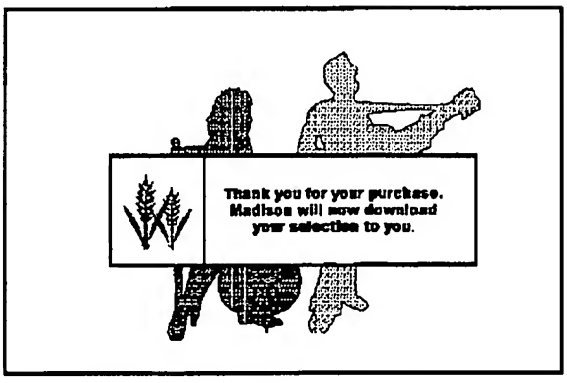
【図１１】


新コンテンツ要求
802
自動メタデータ収集
803
手動メタデータ入力
804
使用条件
805
監視付きリリース
806
メタデータSC作成
807
ウォータマーク
808
前処理圧縮
809
コンテンツ品質管理
810
暗号化
811
コンテンツSC作成
812
813
最終品質保証
814
コンテンツ分散
製品待受けアクション／情報
801
151
メタデータ同化入力ツール
155
コンテンツ処理ツール

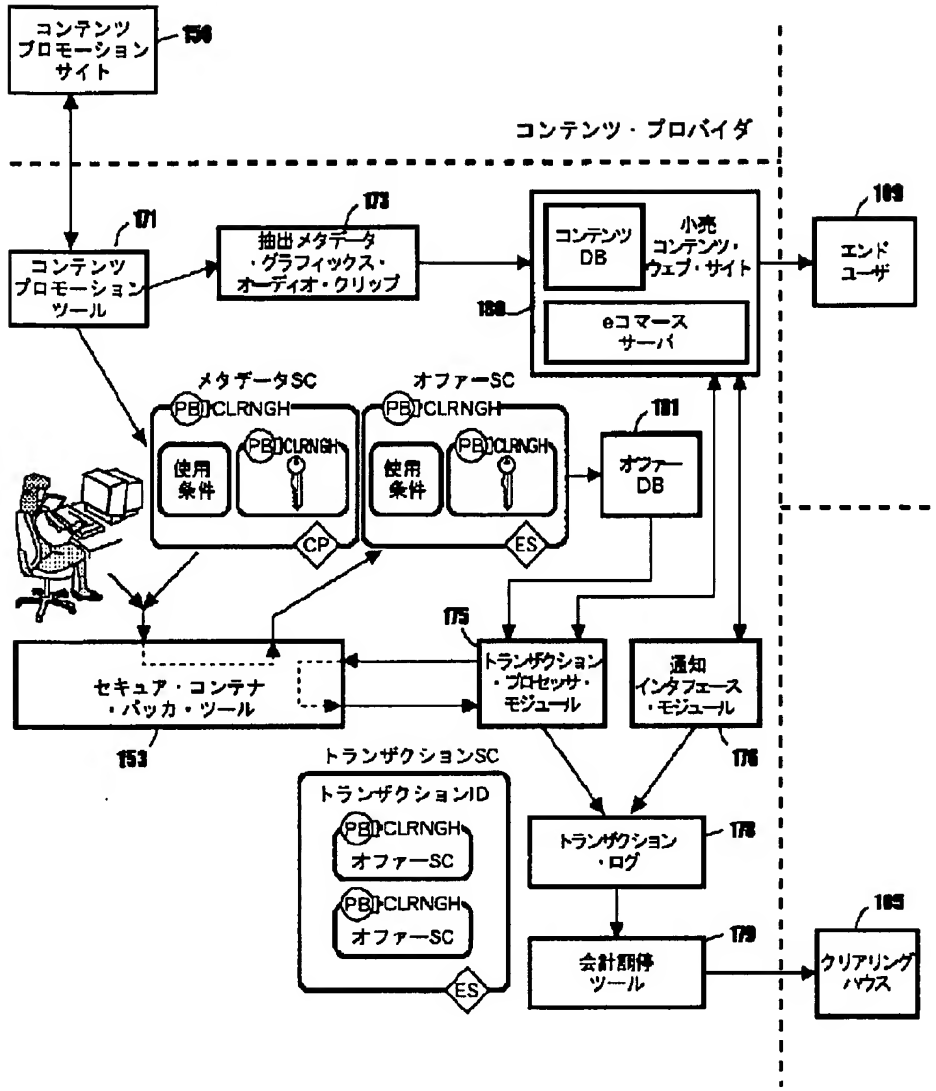
【図２９】


Foodwood Mac
The Dance
$4.50
Back to Previews
Make sure your Smart Card is inserted, and enter your PIN:

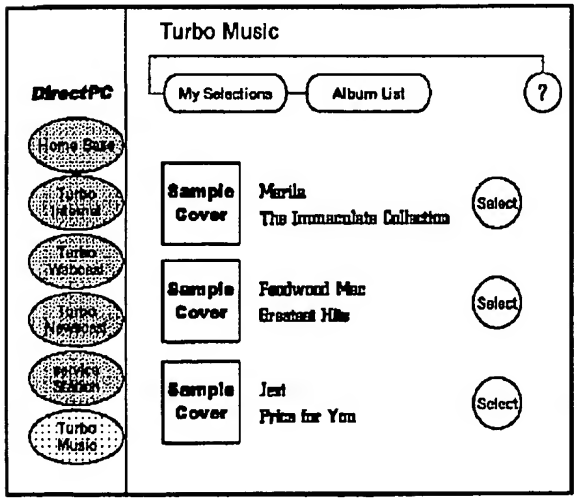
【図３０】


Thank you for your purchase. Madison will now download your selection to you.

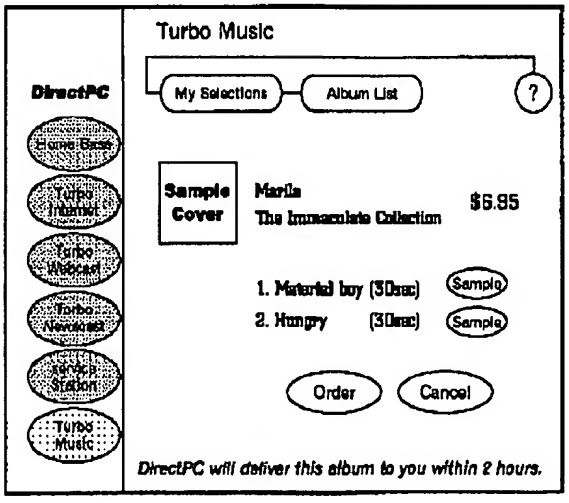
【図１２】


コンテンツ
プロモーション
サイト
150
コンテンツ・プロバイダ
171
コンテンツ
プロモーション
ツール
173
抽出メタデータ
・グラフィックス・
オーディオ・クリップ
コンテンツ
DB
小売
コンテンツ・
ウェブ・サイト
169
エンド
ユーザ
168
eコマース
サーバ
メタデータSC
オファーSC
PBE
CLRNGH
使用
条件
CP
ES
181
オファー
DB
175
トランザクション
・プロセッサ・
モジュール
通知
インタフェース
・モジュール
セキュア・コンテナ
・パッカ・ツール
153
176
トランザクションSC
トランザクションID
オファーSC
178
トランザクション
・ログ
179
会計調停
ツール
185
クリアリング
ハウス

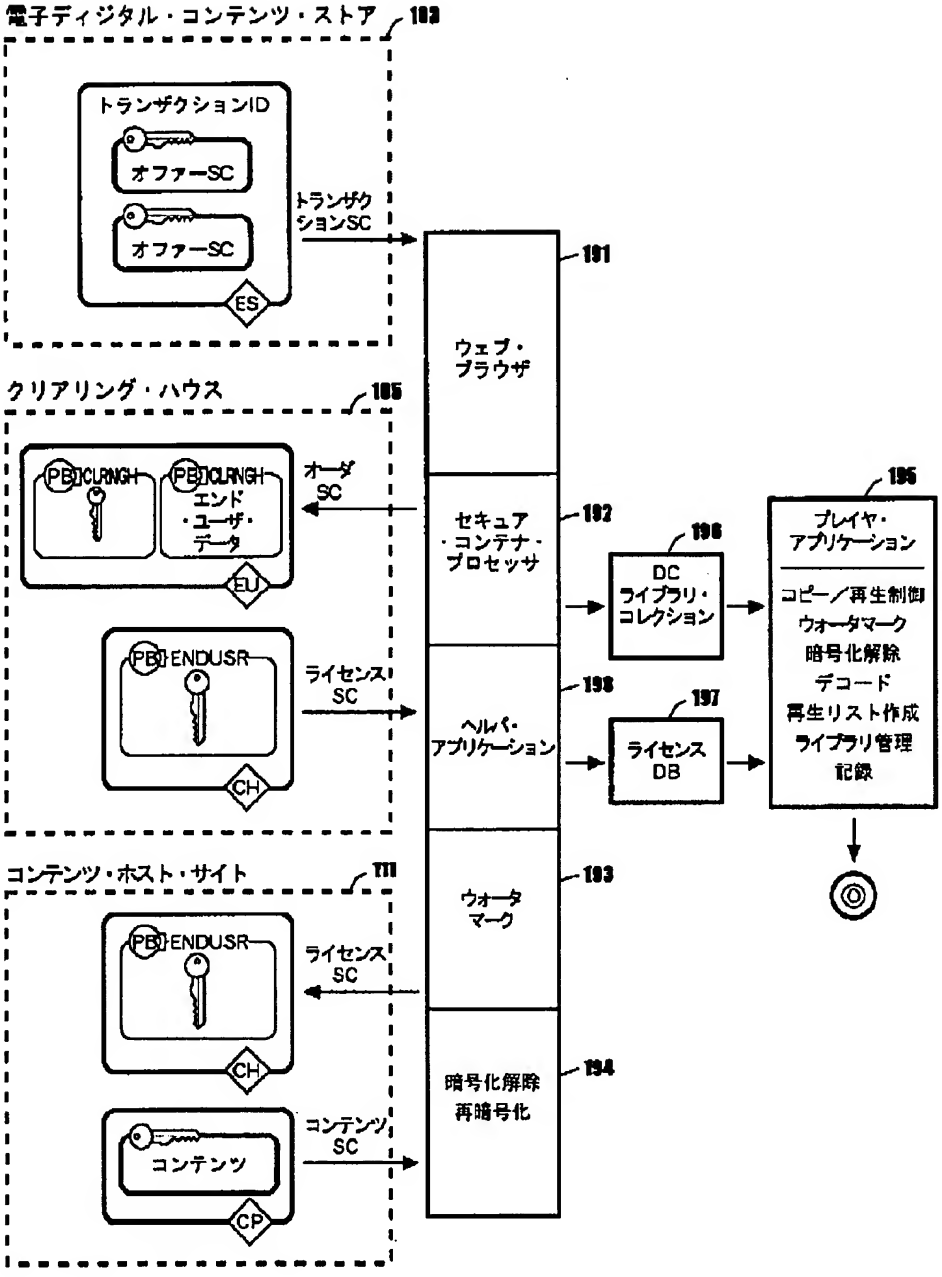
【図３３】


Turbo Music
DirectPC
My Selections
Album List
?
Home Base
Turbo Internet
Turbo Webcast
Turbo Newscast
Service Station
Turbo Music
Sample Cover
Marila
The Immaculate Collection
Select
Sample Cover
Fleetwood Mac
Greatest Hits
Select
Sample Cover
Jet
Price for You
Select

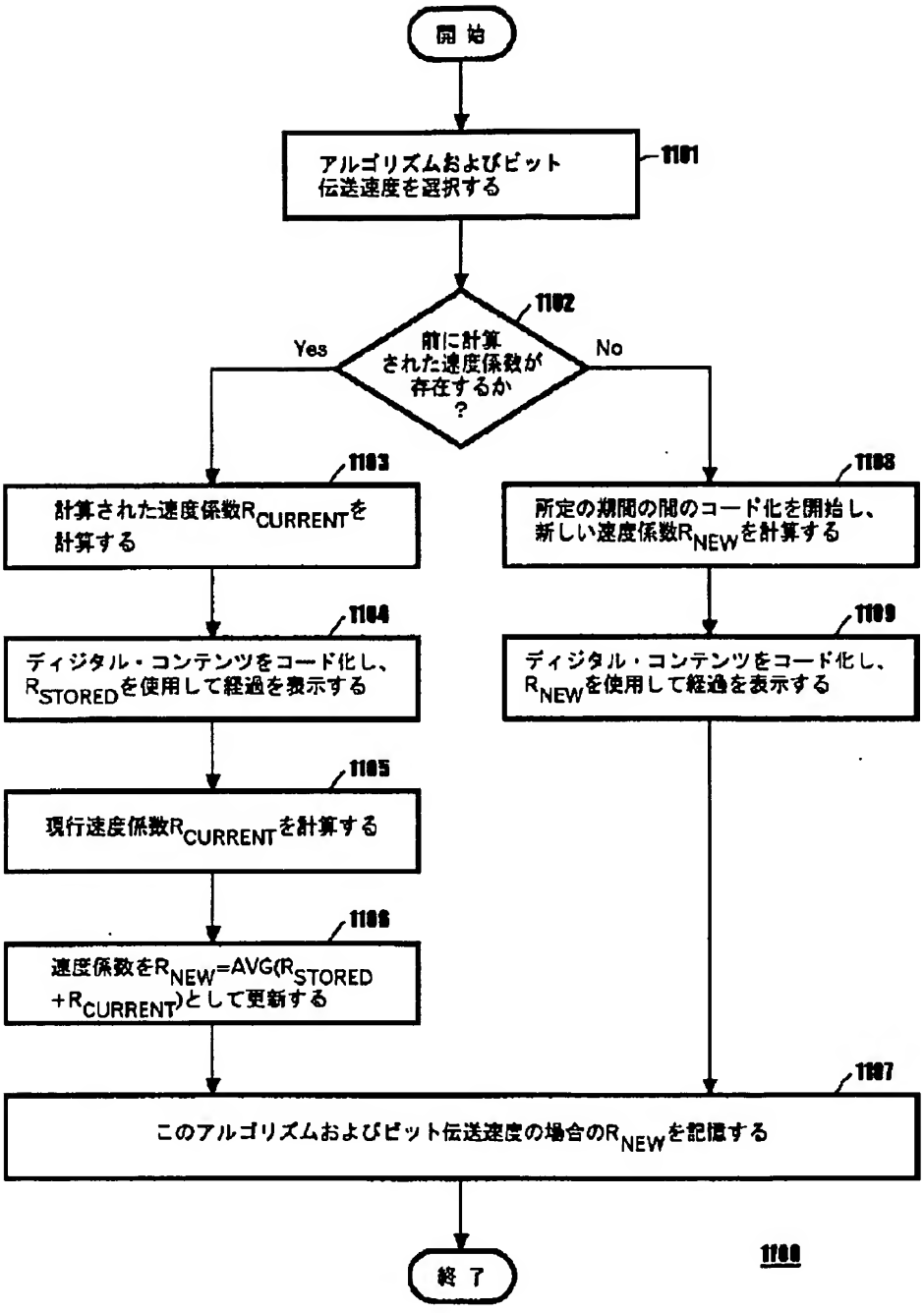
【図３４】


Turbo Music
DirectPC
My Selections
Album List
?
Home Base
Turbo Internet
Turbo Webcast
Turbo Newscast
Service Station
Turbo Music
Sample Cover
Marila
The Immaculate Collection
$6.95
1. Material boy (30sec)
Sample
2. Hungry (30sec)
Sample
Order
Cancel
DirectPC will deliver this album to you within 2 hours.

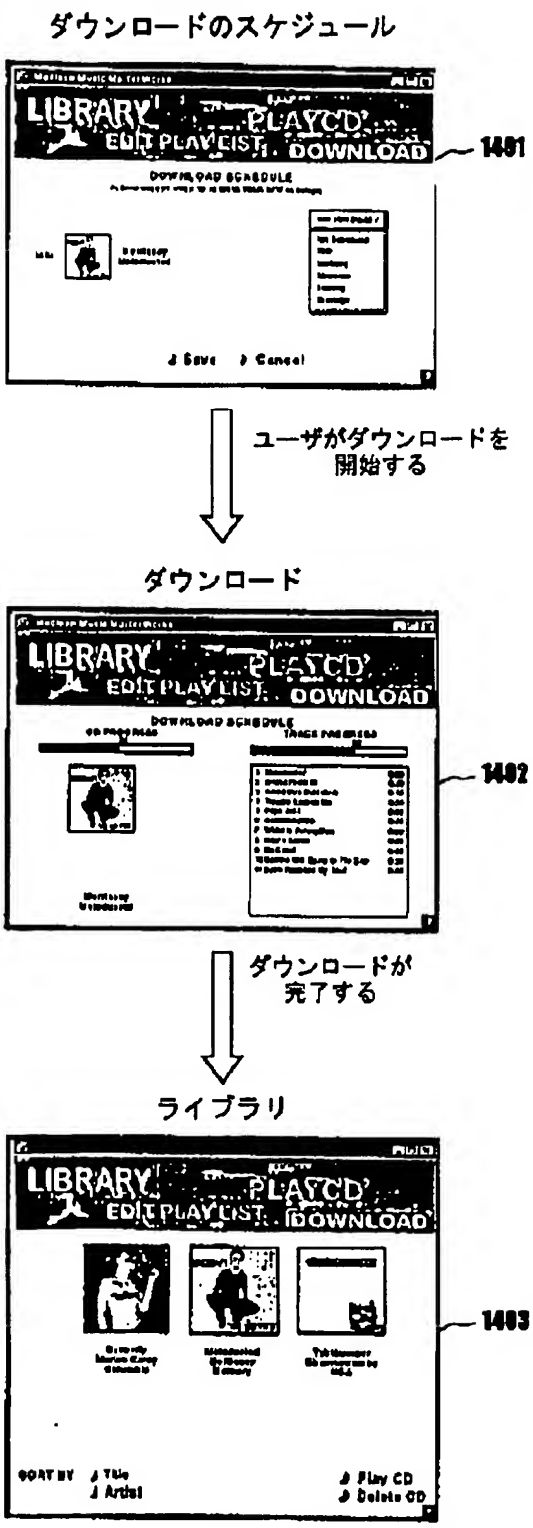
【図１３】


電子ディジタル・コンテンツ・ストア
182
トランザクションID
オファーSC
オファーSC
ES
トランザクションSC
クリアリング・ハウス
185
PB1CLRNGH
PB2CLRNGH
エンド・ユーザ・データ
EU
オーダSC
PB1ENDUSR
CH
ライセンスSC
コンテンツ・ホスト・サイト
111
PB1ENDUSR
CH
ライセンスSC
コンテンツ
CP
コンテンツSC
ウェブ・ブラウザ
191
セキュア・コンテナ・プロセッサ
192
ヘルパ・アプリケーション
193
ウォータマーク
暗号化解除再暗号化
194
DCライブラリ・コレクション
196
ライセンスDB
197
プレイヤ・アプリケーション
195
コピー／再生制御
ウォータマーク
暗号化解除
デコード
再生リスト作成
ライブラリ管理
記録

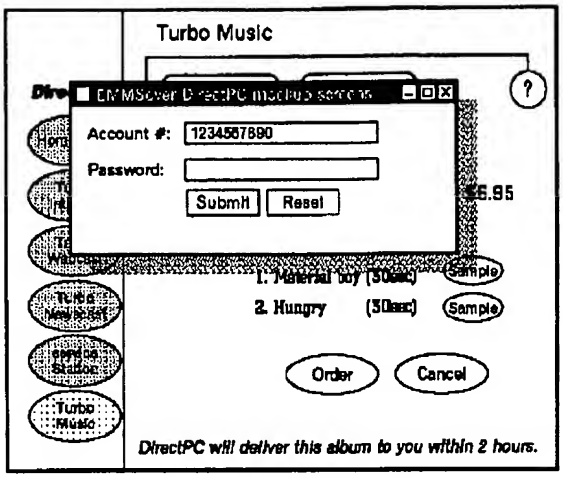
【図１４】


開始
アルゴリズムおよびビット伝送速度を選択する
1101
前に計算された速度係数が存在するか？
1102
Yes
No
計算された速度係数$R_{CURRENT}$を計算する
1103
ディジタル・コンテンツをコード化し、R_{STORED}を使用して経過を表示する
1104
現行速度係数$R_{CURRENT}$を計算する
1105
速度係数をR_{NEW}=AVG(R_{STORED} +$R_{CURRENT}$)として更新する
1106
所定の期間の間のコード化を開始し、新しい速度係数R_{NEW}を計算する
1108
ディジタル・コンテンツをコード化し、R_{NEW}を使用して経過を表示する
1109
このアルゴリズムおよびビット伝送速度の場合のR_{NEW}を記憶する
1107
終了
1100

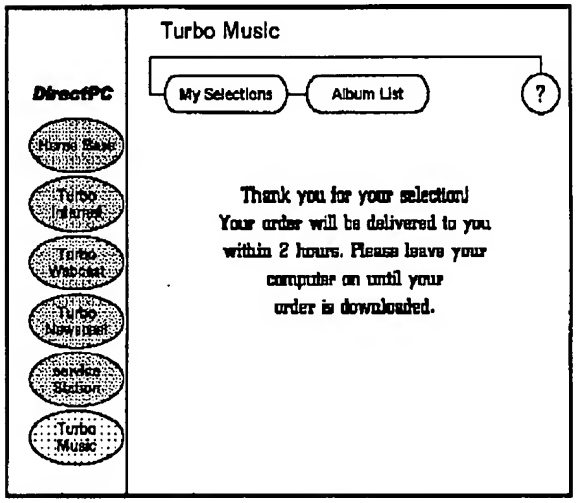
【図１７】



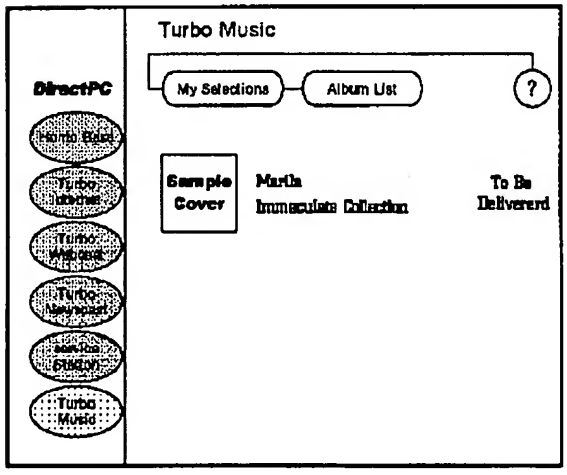
【図３５】



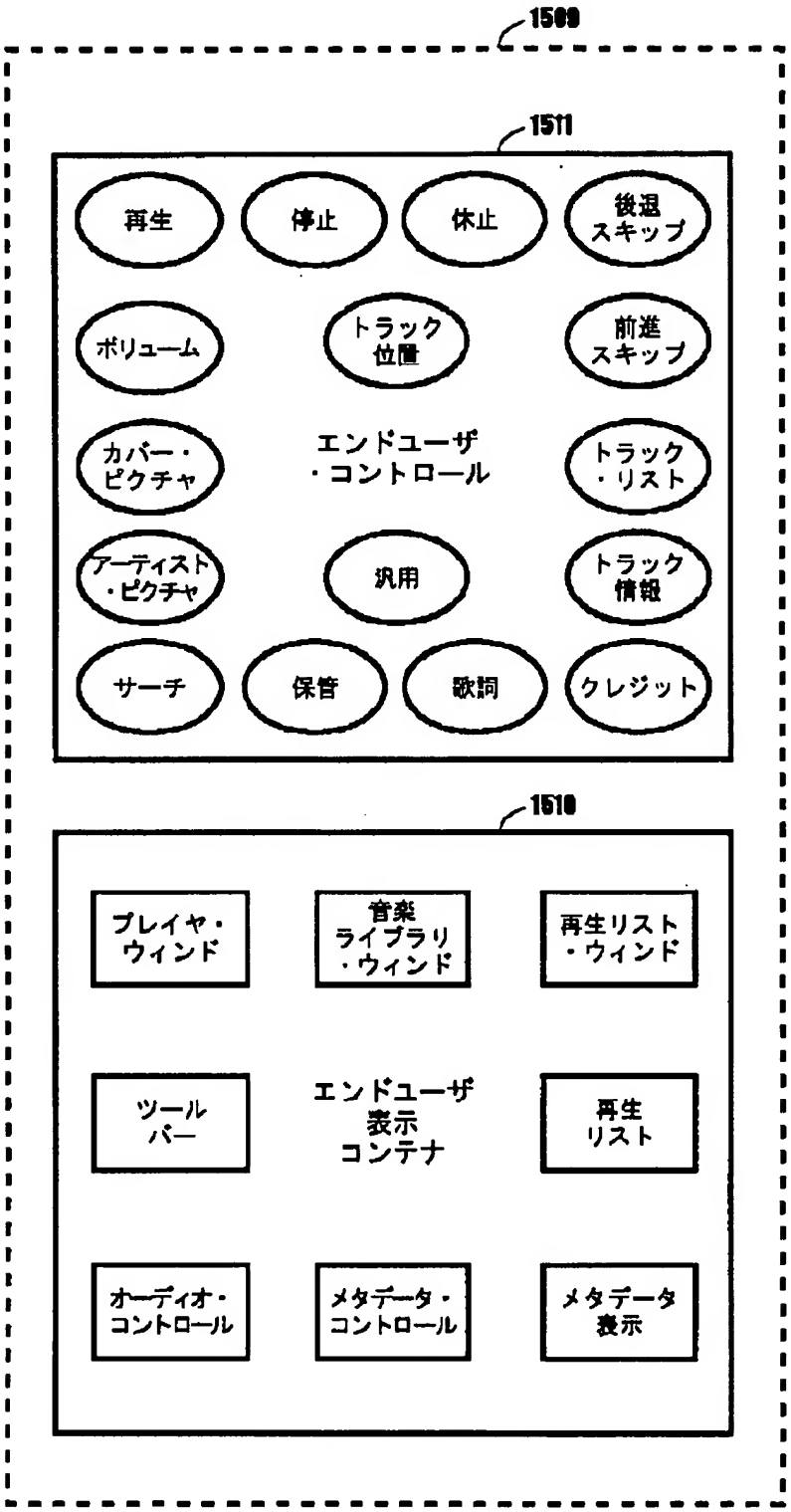
【図３６】



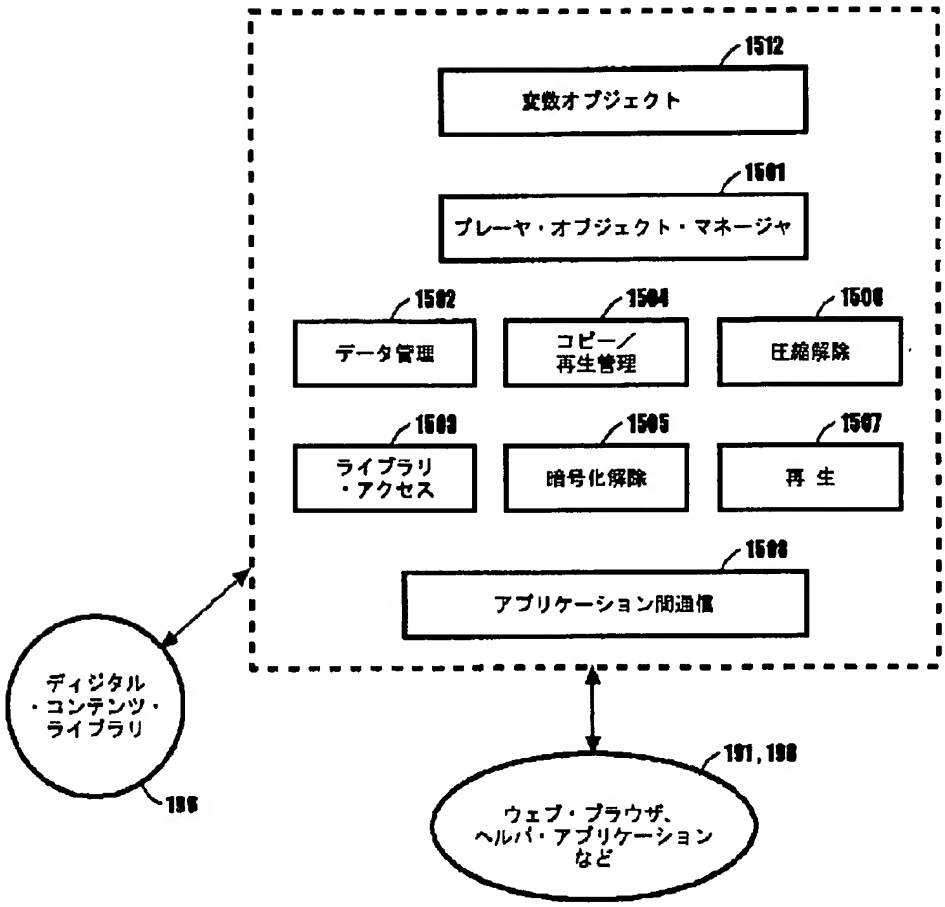
【図３７】



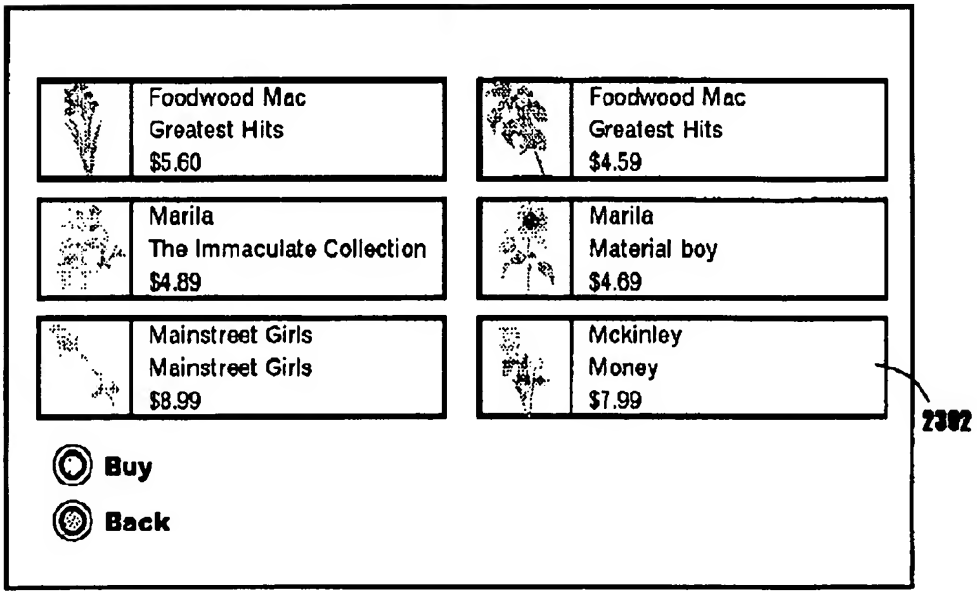
【図１８】


1500
1511
再生
停止
休止
後退
スキップ
ボリューム
トラック
位置
前進
スキップ
カバー・
ピクチャ
エンドユーザ
・コントロール
トラック
・リスト
アーティスト
・ピクチャ
汎用
トラック
情報
サーチ
保管
歌詞
クレジット
1510
プレイヤ・
ウィンド
音楽
ライブラリ
・ウィンド
再生リスト
・ウィンド
ツール
バー
エンドユーザ
表示
コンテナ
再生
リスト
オーディオ・
コントロール
メタデータ・
コントロール
メタデータ
表示

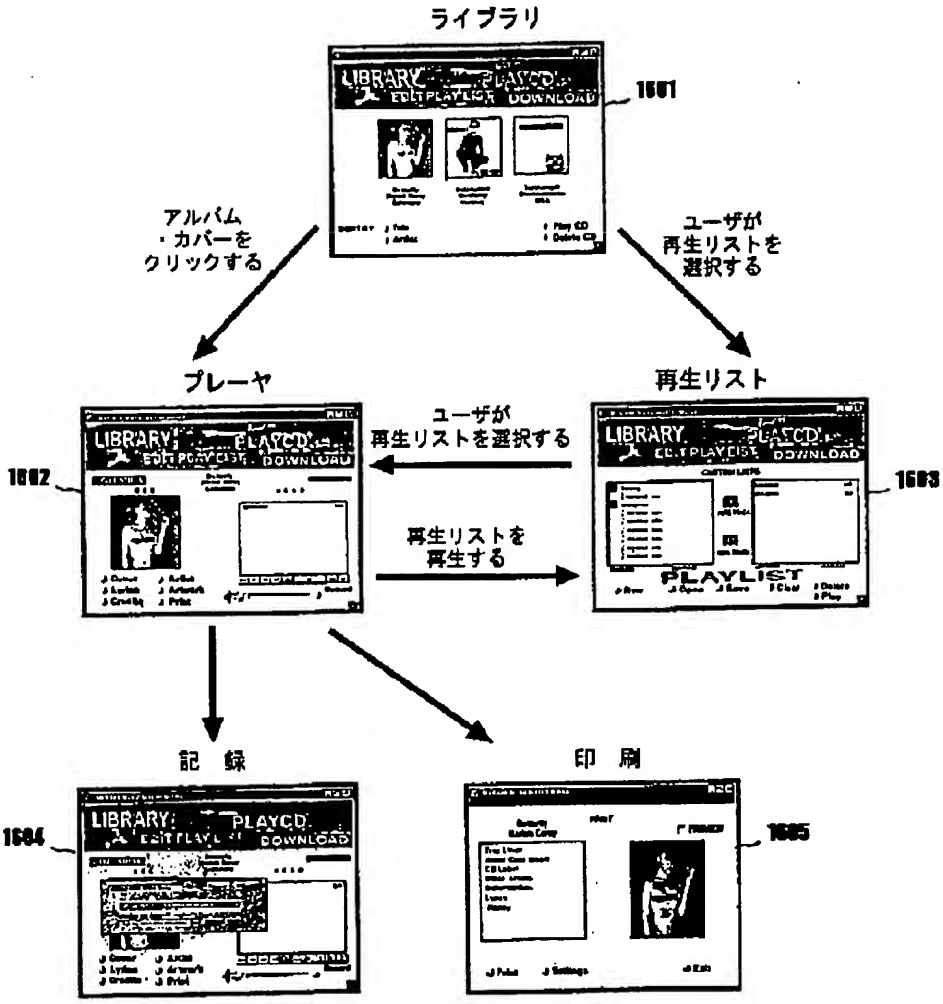
【図１９】


1512
変数オブジェクト
1501
プレーヤ・オブジェクト・マネージャ
1502
データ管理
1504
コピー／
再生管理
1506
圧縮解除
1503
ライブラリ
・アクセス
1505
暗号化解除
1507
再 生
1508
アプリケーション間通信
ディジタル
・コンテンツ・
ライブラリ
186
191, 193
ウェブ・ブラウザ、
ヘルパ・アプリケーション
など

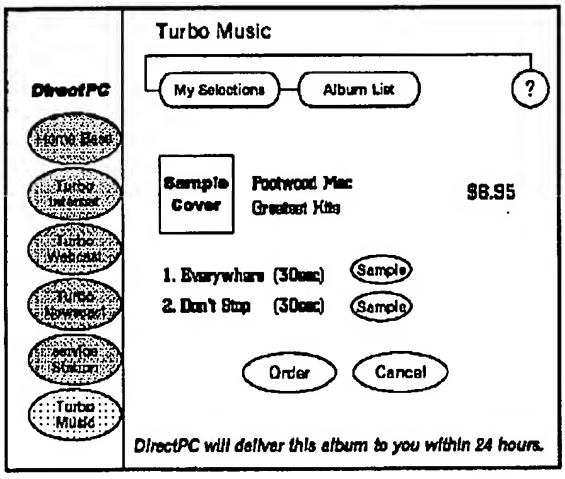
【図２７】


Foodwood Mac
Greatest Hits
$5.60
Foodwood Mac
Greatest Hits
$4.59
Marila
The Immaculate Collection
$4.89
Marila
Material boy
$4.69
Mainstreet Girls
Mainstreet Girls
$8.99
Mckinley
Money
$7.99
2302
Buy
Back

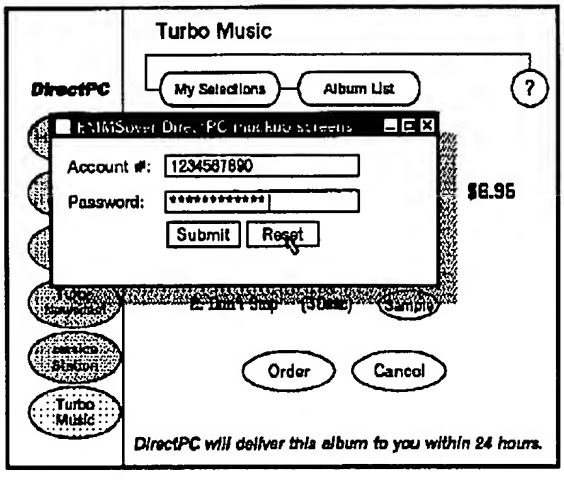
【図２０】


ライブラリ
1681
アルバム
・カバー
をクリックする
ユーザが
再生リストを
選択する
プレーヤ
再生リスト
ユーザが
再生リストを選択する
1682
1683
再生リストを
再生する
記　録
印　刷
1684
1685

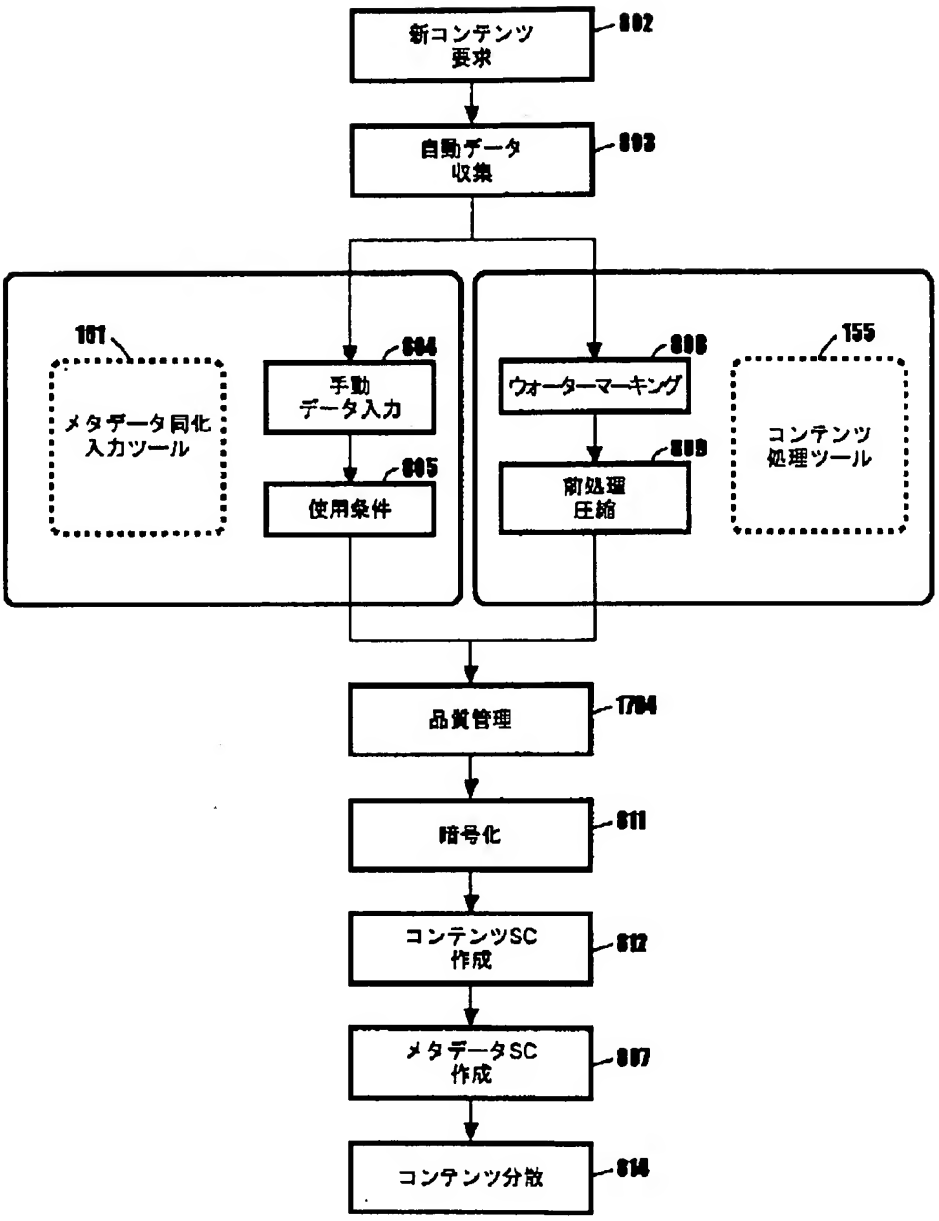
【図３８】


Turbo Music
DirectPC
My Selections
Album List
?
Sample Cover
Fleetwood Mac
Greatest Hits
$8.95
1. Everywhere (30sec)
Sample
2. Don't Stop (30sec)
Sample
Order
Cancel
DirectPC will deliver this album to you within 24 hours.

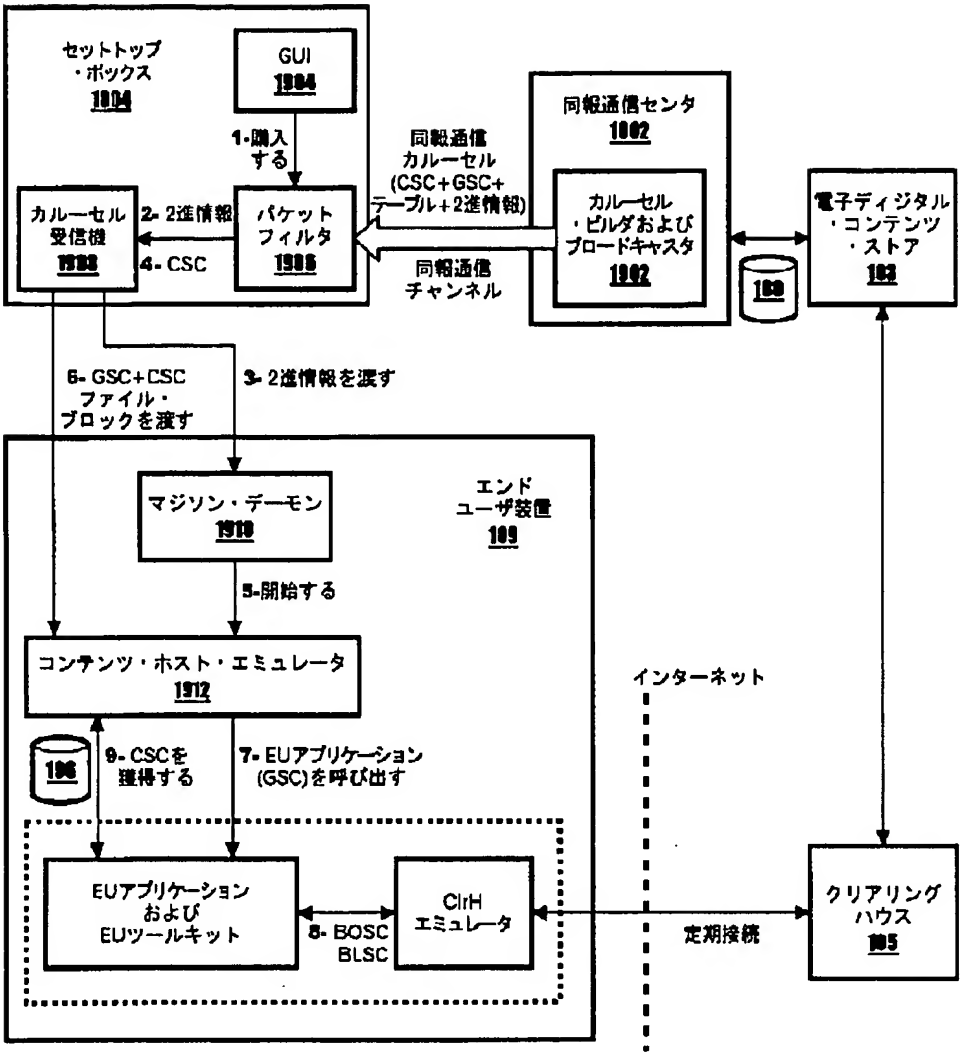
【図３９】


Turbo Music
DirectPC
My Selections
Album List
?
Account #:
1234567890
Password:
Submit
Reset
$8.95
Order
Cancel
DirectPC will deliver this album to you within 24 hours.

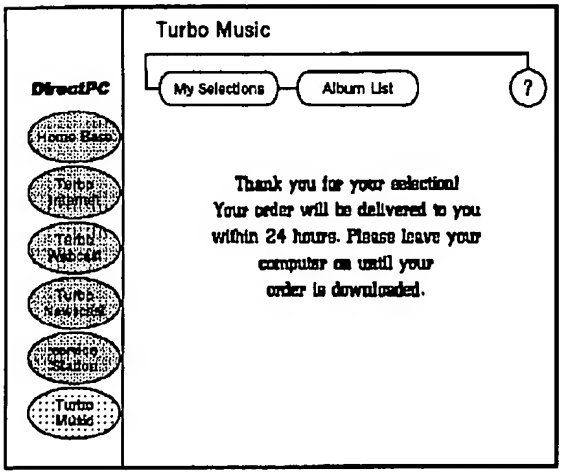
【図２１】


新コンテンツ要求
802
自動データ収集
803
101
メタデータ同化入力ツール
804
手動データ入力
805
使用条件
806
ウォーターマーキング
809
前処理圧縮
155
コンテンツ処理ツール
品質管理
1704
暗号化
811
コンテンツSC作成
812
メタデータSC作成
807
コンテンツ分散
814

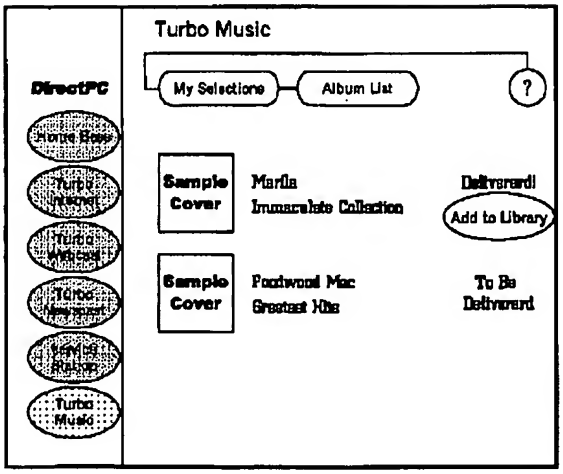
【図２３】


セットトップ
・ボックス
1004
GUI
1004
1-購入する
同報通信センタ
1002
同報通信
カルーセル
(CSC+GSC+
テーブル+2進情報)
カルーセル
受信機
1008
2- 2進情報
4- CSC
パケット
フィルタ
1006
カルーセル
・ビルダおよび
ブロードキャスタ
1002
同報通信
チャンネル
160
電子ディジタル
・コンテンツ
・ストア
102
6- GSC+CSC
ファイル・
ブロックを渡す
3- 2進情報を渡す
マジソン・デーモン
1010
エンド
ユーザ装置
100
5-開始する
コンテンツ・ホスト・エミュレータ
1012
インターネット
106
9- CSCを
獲得する
7- EUアプリケーション
(GSC)を呼び出す
EUアプリケーション
および
EUツールキット
8- BOSC
BLSC
ClrH
エミュレータ
定期接続
クリアリング
ハウス
105

【図４０】

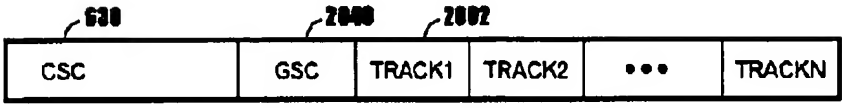

Turbo Music
DirectPC
My Selections
Album List
?
Thank you for your selection!
Your order will be delivered to you
within 24 hours. Please leave your
computer on until your
order is downloaded.

【図４１】


Turbo Music
DirectPC
My Selections
Album List
?
Sample
Cover
Marilla
Immaculate Collection
Delivered!
Add to Library
Sample
Cover
Fleetwood Mac
Greatest Hits
To Be
Delivered

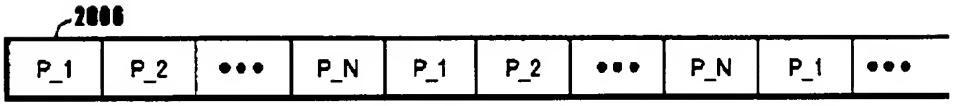
【図２４】

パッケージ・フォーマット



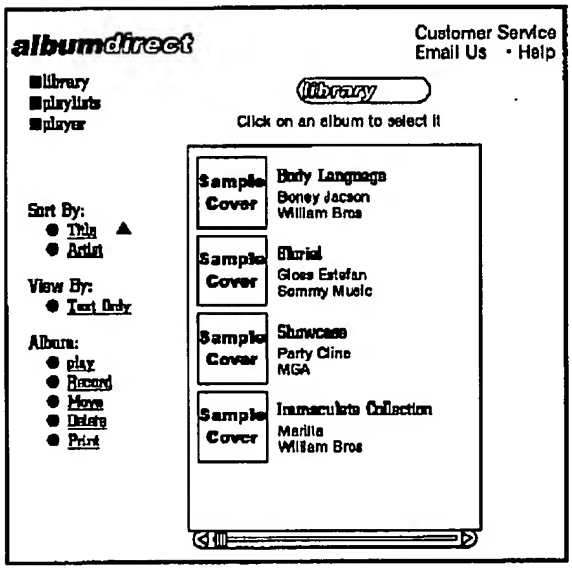
CSC = コンテンツ・セキュア・コンテナ
GSC = グローバル・セキュア・コンテナ、
すなわち、各ユーザに毎週配布されるグローバル・キーを使用して
暗号化されたキーを備えたセキュア・コンテナ
ASCはアート・ワーク・セキュア・コンテナである

カルーセル・フォーマット

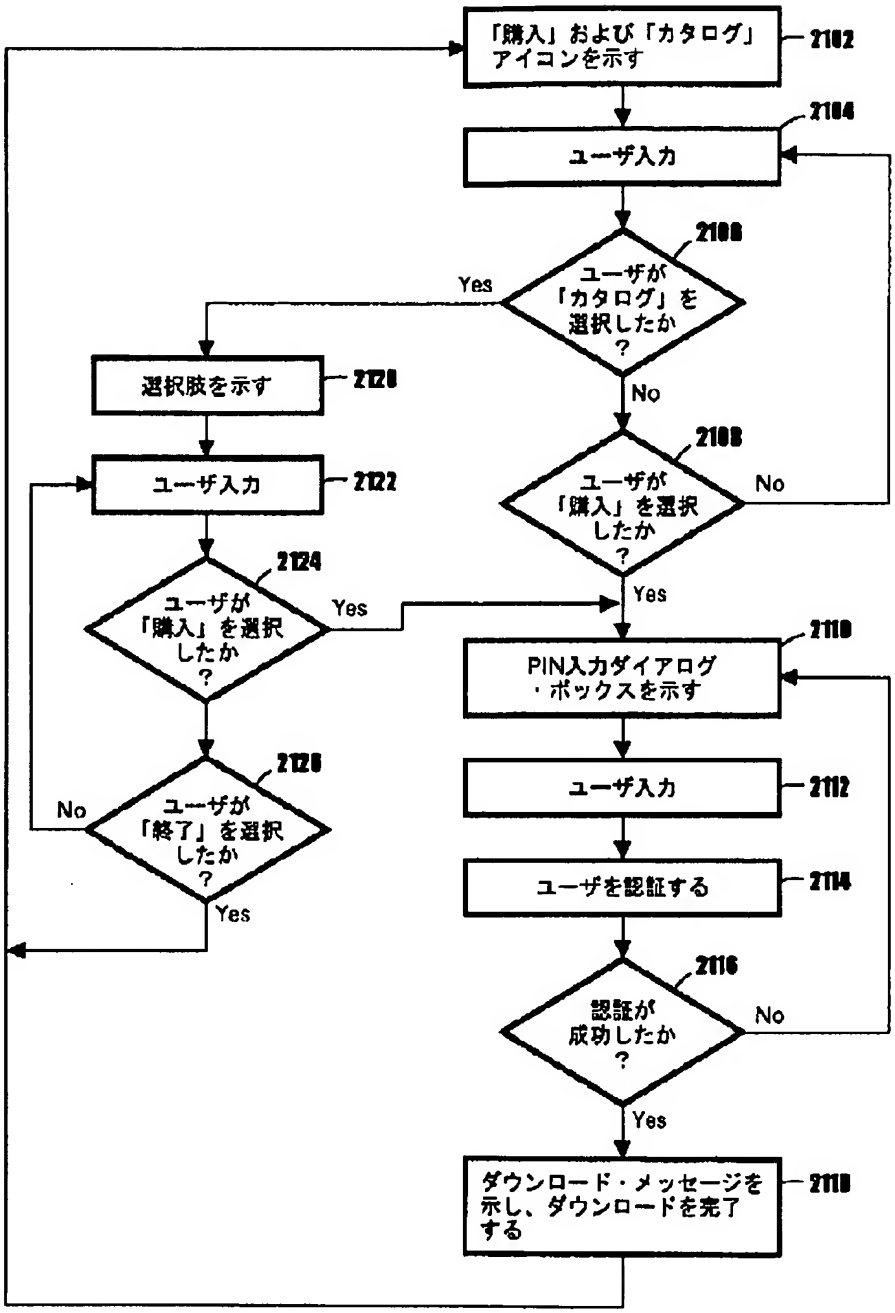


パッケージは、カルーセル方式で同報通信チャネルにより、伝送される
カルーセルは、定期的に繰り返し現れる循環構造である
P_1 = パッケージ #1
P_2 = パッケージ #2
P_N = パッケージ #N

【図４２】

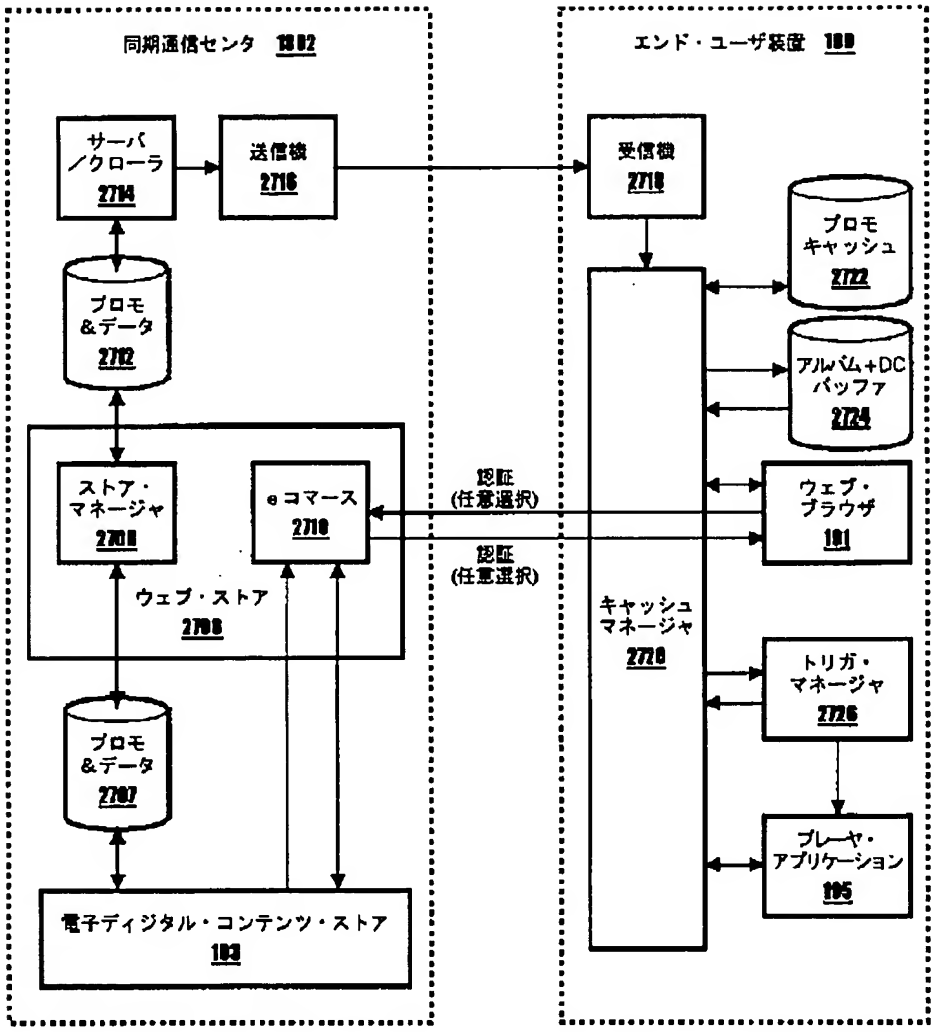


【図２５】

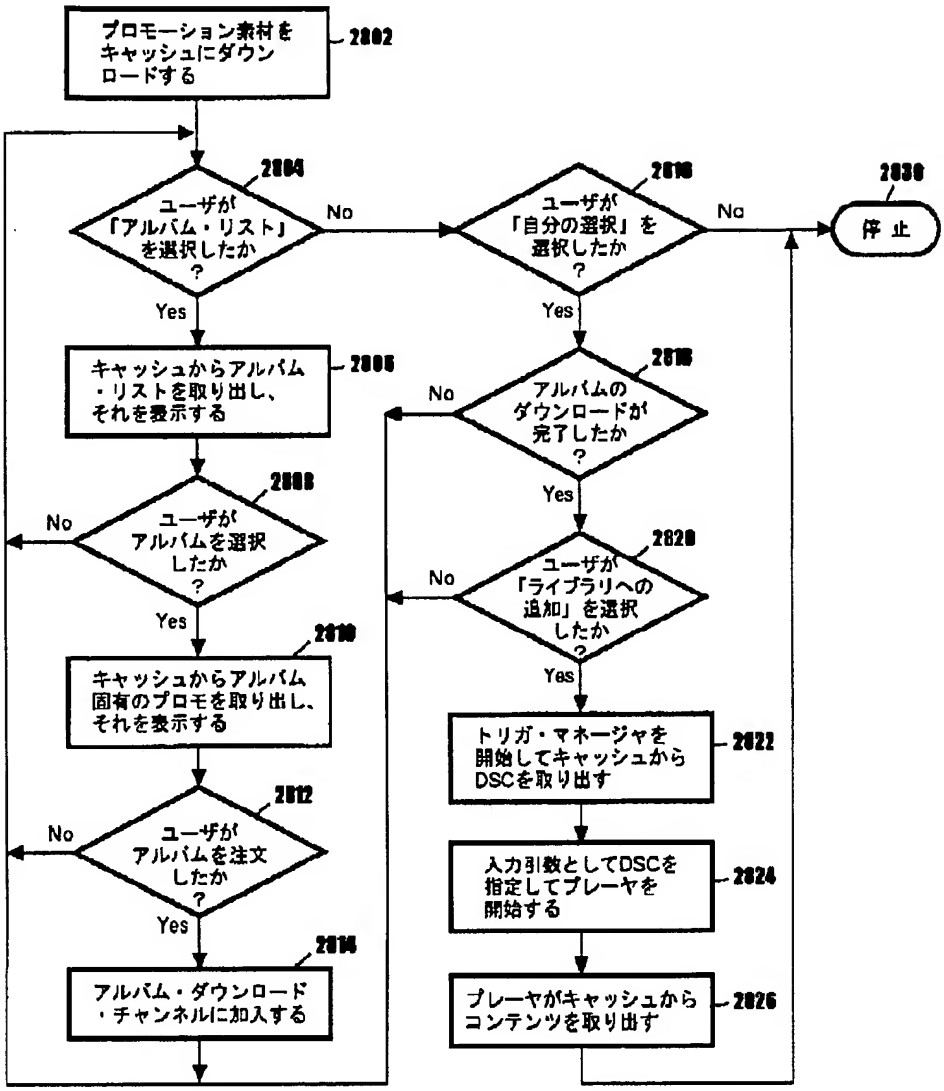

「購入」および「カタログ」アイコンを示す
2102
2104
ユーザ入力
2106
ユーザが「カタログ」を選択したか？
Yes
No
選択肢を示す
2120
ユーザ入力
2122
2108
ユーザが「購入」を選択したか？
No
Yes
2124
ユーザが「購入」を選択したか？
Yes
2110
PIN入力ダイアログ・ボックスを示す
2126
ユーザが「終了」を選択したか？
No
Yes
ユーザ入力
2112
ユーザを認証する
2114
2116
認証が成功したか？
No
Yes
ダウンロード・メッセージを示し、ダウンロードを完了する
2118

2100

【図３１】


同期通信センタ 1002
エンド・ユーザ装置 100
サーバ／クローラ 2714
送信機 2716
受信機 2718
プロモ&データ 2702
プロモキャッシュ 2722
アルバム+DCバッファ 2724
ストア・マネージャ 2708
eコマース 2710
認証(任意選択)
認証(任意選択)
ウェブ・ブラウザ 101
ウェブ・ストア 2706
キャッシュマネージャ 2720
トリガ・マネージャ 2726
プロモ&データ 2707
プレーヤ・アプリケーション 105
電子ディジタル・コンテンツ・ストア 103

【図３２】



フロントページの続き

(51) Int.Cl.[7]	識別記号	FI	テーマコード（参考）
		H04L 9/00	601E

(72)発明者 マグダ・マウラド
アメリカ合衆国10598 ニューヨーク州ヨークタウン・ハイツ チェスナット・コート 397

(72)発明者 ジョナサン・ピー・マンソン
アメリカ合衆国10579 ニューヨーク州パトナム・ヴァレイ クレイマーズ・ポンド・ロード 24

(72)発明者 ジョヴァンニ・パチフィチ
アメリカ合衆国10024 ニューヨーク州ニューヨーク ウェスト・エイティー・ファースト・ストリート・ナンバー14 101

(72)発明者 アフメド・タンタウィー
アメリカ合衆国10598 ニューヨーク州ヨークタウン・ハイツ チェスナット・コート 397

(72)発明者　アラー・エス・ユーセフ
アメリカ合衆国10535　ニューヨーク州ジェファーソン・ヴァレイ　イースト・メイン・ストリート620　アパートメント５ディー